韓國컴퓨터情報學會 論文誌
第14卷 第12號, 2009. 12.

2009-14-12-1-1

MGrid에서 그리드 포털과 웹 어플리케이션의 통합인증

허 대 영*, 황 대 복**, 황 선 태***

Single Sign On between Grid Portal and Web applications on MGrid

Daeyoung Heo*, Daebok Hwang**, Suntae Hwang***

요 약

그리드 서비스는 X.509 대칭키 기반의 GSI(Grid Security Infrastructure) 환경으로 통합 인증 하는 반면에 웹 환경에서는 계정 이름과 비밀번호를 사용한 인증 방식으로 통합 인증을 한다. 그리드 포털은 그리드 서비스를 포틀릿 콘텐츠로 통합하여, 웹 환경에서 그리드 서비스를 제공하는 시스템을 말하는 데, GAMA, PURSE와 같은 기존의 연구를 보면 전면에서는 계정 이름과 비밀번호를 사용해서 인증하고, 후면에서는 GSI 기반으로 그리드 서비스를 호출하는 방식으로 통합 인증을 해결하였다. 기존의 연구에서는 포틀릿 프레임워크 안에서의 통합 인증만 다루고 있으므로 포틀릿 프레임워크를 벗어난 다른 형태의 어플리케이션으로는 그리드 서비스에 통합 인증으로 접근할 수 없다. 본 논문에서는 계정 이름과 비밀번호의 사용을 기본으로 하되, 인증된 정보와 그리드로 접근할 때 사용할 GSI 토큰을 포틀릿과 다른 웹 어플리케이션들 사이에 전달하는 방식의 통합 인증을 제안하였다. 본 논문에서 제시한 방안을 포틀릿 뿐만아니라 자바 웹 스타트, 애플릿 및 서블릿 등으로 구성된 MGrid에 통합 인증을 위하여 적용하였다.

Abstract

Grid services offer SSO(single sign-on) mechanism using GSI(grid security infrastructure) based on X.509. However, portal applications in web environment use ID and password model for single sign-on. Grid portals means a system which provides grid services by integrating portlet contents on single web interface. In existing research such as GAMA and PURSE, SSO for a whole grid portal is figured out in the way that user is authenticated by ID and password in front and call grid service via GSI at back-end. Other types of web applications outside of portlet framework cannot unfortunately access grid service in SSO way in the existing researches, because the SSO mechanism is developed for portlet framework only. In this paper, we suggest a SSO mechanism based on ID and password model, which forwards authentication information and a GSI token for grid access among portlets and grid-enabled web applications. This mechanism is applied to MGrid for SSO, which consists of applications of java web start, applet, servlet, and etc. as also as portlets.

▸ Keyword : MGrid, 통합 인증(MGrid, Single Sign On), 그리드 포털(Grid Portal), 웹 어플리케이션(Web applications), 그리드 시큐리티(Grid Security)

• 제1저자 : 허대영 교신저자 : 황선태
• 투고일 : 2009. 03. 25, 심사일 : 2009. 04. 21, 게재확정일 : 2009. 12. 24.
* 국민대학교 일반대학원 전산과학과 박사과정 ** NHN Corp
*** 국민대학교 전자정보통신대학 컴퓨터공학부 교수
※ 본 논문은 2008년도 국민대학교 교내 연구비를 지원받아 수행된 연구입니다.

Ⅰ. 서 론

최근 포털 시스템이 그리드 환경의 사용자 인터페이스로 많이 이용되고 있다. 사용자가 그리드 미들웨어의 설치 없이 손쉽게 그리드 환경을 이용할 수 있다는 장점으로 인해 그리드 포털에 관한 연구가 활발하다. 대표적인 예로 그리드스피어[1] 의 GridPortlet[2] 과 OGCE[3] 의 GridPort[4] 프로젝트가 있다.

그리드는 네트워크를 기반으로 공유되는 분산된 자원의 보안과 저장되는 데이터의 보호가 중요하기 때문에 공개키와 개인키로 이루어진 대칭키를 기반으로 한 보안메커니즘을 사용한다. 그러나 전통적인 포털 시스템은 계정 이름과 패스워드를 사용자 인증으로 사용한다. 이와 관련하여 포털 시스템의 사용자 계정과 그리드 서비스의 대칭키의 맵핑 관계를 중심으로 포털과 그리드 시스템의 통합에 대한 많은 연구가 진행 중이다. 특히 GAMA[5] (Grid Account Management Architecture)와 PURSE[6](Portal-Based User Registration Service) 처럼 계정 이름, 패스워드 방식에 익숙한 사용자의 편의성에 초점을 둔 연구가 주목받고 있다.

포털 시스템인 포틀릿 프레임워크가 그리드 환경의 사용자 인터페이스로 대두되면서, 그리드 서비스를 위한 응용들이 웹 어플리케이션형태로 제공되고 있다. 사용자는 그리드 포털에서 제공하는 웹 어플리케이션을 이용하기 위해서 포털과 웹 어플리케이션에서 각각의 사용자 인증과정이 필요하다.

통합 인증기능은 사용자가 처음 한 번의 사용자 인증 후에 추가적인 인증과정 없이 허가된 권한 내에서 그리드 자원들을 이용 할 수 있도록 하는 것이다.

GAMA는 포털 간의 사용자 계정 정보 내보내기, 가져오기 기능을 통해 포털 수준의 통합인증을 지원한다. 이는 포틀릿 프레임워크에서 통합인증을 수행함으로써 포틀릿이 아닌 웹 어플리케이션과 포탈 또는 여러 독립적인 웹 어플리케이션 사이의 통합인증은 어렵다고 할 수 있다. 따라서 본 논문에서는 그리드 포털과 포털 독립적인 웹 어플리케이션, 여러 독립적인 웹 어플리케이션 사이의 통합인증을 위한 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문의 연구결과를 적용시킨 MGrid [7][8][9] 프로젝트와 MGrid 시스템의 보안요구사항을 소개한다. 3장에서는 MGrid-security 의 설계와 구현에 대해 설명한다. 4장에서는 MGrid-security를 평가한다. 마지막으로 5장에서는 결론과 함께 향후 연구계획을 언급하고 마무리한다.

Ⅱ. MGrid 시스템과 보안 요구사항

2.1 MGrid 시스템

MGrid (Molecular Simulation Grid) 프로젝트는 초기 그리드 환경에서 분자시뮬레이션을 효과적으로 지원하기 위한 소프트웨어개발 과제로 시작하여 이후 이 소프트웨어를 적용하여 실제 분자시뮬레이션 작업을 서비스할 수 있는 그리드 인프라를 구축하였다. 초기에는 분자 시뮬레이션 작업 서비스에 초점을 둔 컴퓨팅 그리드 개발 중심에서 최근에는 분자시뮬레이션 실험데이터 및 이의 공유에 초점을 둔 데이터 그리드 개발에 역점을 두어 진행되고 있다.

MGrid는 분자 시뮬레이션 연구를 위한 계산 그리드와 데이터 그리드 간의 효율적인 공유를 목표로 MGrid-CG, MGrid-PSE, MGrid-SDG로 구성되어 있다. MGrid를 기반으로 특정 분야를 위한 MGrid 응용을 구축할 수 있는데 현재 Glyco-MGrid가 있다.

MGrid 시스템의 UI 계층은 추상화된 사용자 인터페이스인 MGrid 포털, Glyco-MGrid 포털을 비롯하여, 시뮬레이션 작업들에 대한 상호작용 가능한 모니터링을 제공하고 연구자들에게 관련 결과 파일들에 대한 분석과 시각화 기능을 제공하는 웹 어플리케이션들로 구성되어 있다. MGrid에서 제공하는 웹 어플리케이션들은 포털 독립적이기 때문에 MGrid UI 계층의 여러 포털에서 호출될 수 있다.

MGrid의 서비스 계층은 분자 시뮬레이션의 수행과 분석에 필요한 서비스들과 실험결과와 메타데이터들의 저장과 검색에 필요한 시맨틱 데이터 그리드 서비스들로 구성되어 있다. MGrid의 구성요소는 그림 1에 나타나 있다.

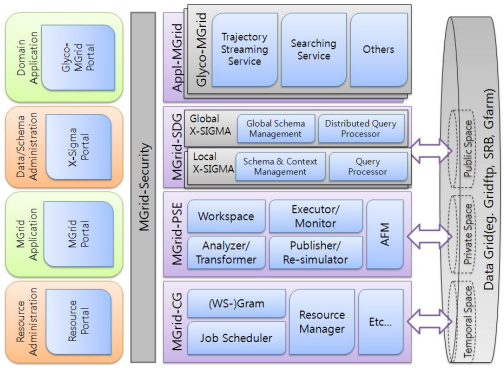

그림 1. MGrid 시스템 구성요소
Fig. 1 MGrid System Components

2.2 MGrid 시스템의 보안 요구사항

MGrid의 사용자 인터페이스를 담당하는 여러 포털과 웹 어플리케이션들은 사용자 인증뿐 아니라 포털과 각 웹 어플리케이션 사이의 통합인증이 필요하다. 시스템 보안 및 사용자 인증 관점에서 보안 요구사항은 다음과 같다.

1) 사용자 등록과정과 사용자계정

MGrid 시스템은 공개 시스템이 아니라 분자 시뮬레이션 연구를 위한 컴퓨팅 자원과 실험결과와 같은 중요한 데이터들을 공유하는 시스템이다. 따라서 사용자 등록이 필수적이다.

2) UI 계층의 접근 제한

MGrid의 UI 계층은 여러 포털과 웹 어플리케이션들로 구성되어 있다. 사용자에게 허가된 권한에 따라 접근 및 사용이 가능한 포털과 웹 어플리케이션들이 구분되어야 한다.

3) 서비스 계층에서의 사용자 식별

사용자에게 허가된 권한에 따라 MGrid의 서비스 계층에서 제공하는 그리드 서비스들이 구분되어야 하는데 이를 위해 사용자의 식별이 필요하다.

4) 웹 어플리케이션 사용자 인증

MGrid에서 제공하는 다양한 웹 어플리케이션들은 사용자 권한에 따라 사용이 가능하다. 따라서 포털에 등록된 사용자는 각 웹 어플리케이션을 사용하기 위해 인증과정이 필요하다.

5) 포털과 웹 어플리케이션사이의 통합인증

사용자가 포털에 로그인 한 후에 추가 로그인 과정 없이 웹 어플리케이션들을 이용할 수 있어야 한다. 분자 시뮬레이션에 요구되는 작업들은 많은 컴퓨팅 자원과 시간을 필요로 하기 때문에, 과학자들이 시뮬레이션에서 각 과정 별로 필요한 웹 어플리케이션을 사용할 때마다 로그인한다는 것은 비현실적이다.

6) 웹 어플리케이션 간 통합인증

분자 시뮬레이션 연구를 위해 Charmm, Gaussian 과 같은 레거시 소프트웨어들을 사용한다. 이러한 소프트웨어에 대한 접근을 위해 웹 어플리케이션이 제공되는 데 각 웹 어플리케이션은 관련 결과 파일들에 대한 분석과 시각화, 그리고 재실험을 위해 다른 웹 어플리케이션들을 사용 할 수 있다. 하나의 웹 어플리케이션이 다른 웹 어플리케이션을 사용 할 때 추가적인 사용자 인증 없이 이용하기 위해 통합인증기능이 필요하다.

III. MGrid-security의 설계 및 구현

3.1 전제 조건

본 논문에서는 다음 사항을 전제로 MGrid-security 를 구축하였다.

1) 그리드서비스를 이용하기 위한 포털 존재

그리드 서비스를 이용하기 위한 사용자 인터페이스로 그리드 포털이 존재하며, 이는 그리드 서비스와 플랫폼 독립적이다.

2) 사용자 계정은 포털 계정

사용자 계정은 포털 계정이고, UI 계층에서의 사용자 인증은 포털 계정을 사용한다. 그리드 서비스 계층에서 필요한 대칭키는 UI 계층의 포털 계정과 인증서의 1:1 사상으로 해결한다.

3) 웹 어플리케이션 이용을 위한 포털 로그인

사용자 인증은 포털 계정을 기준으로 하기 때문에 웹 어플리케이션을 이용하기 위해서 사용자는 포털에 로그인해야 한다.

4) 통합인증의 기준은 포털 계정

포털과 웹 어플리케이션, 웹 어플리케이션과 웹 어플리케이션 간의 통합인증은 포털 계정을 기준으로 수행한다.

3.2 사용자 계정관리

MGrid 는 분자 시뮬레이션 연구를 위한 그리드 시스템으로 포털의 사용자 계정을 기준으로 한 사용자 인증과 허가, 그리고 포털과 포털 독립적인 웹 어플리케이션사이의 통합인증기능이 필요하다.

2.2 절에서 언급한 MGrid 시스템의 보안 요구사항 중 "사용자 등록과정과 사용자 계정", "UI 계층의 접근 제한" 요구사항을 해결하기 위해 그리드스피어로 구축한 포털들에 GAMA를 적용하였다.

그리드스피어는 포틀릿 기반의 프레임워크로 각 서비스 별로 재사용이 가능하도록 구현되었으며 사용자 관리, 세션 관리, 그룹 관리, 레이아웃 관리 기능 등을 제공함으로써 사용자가 포털을 통해 그리드 서비스를 쉽게 이용할 수 있도록 한다.

GAMA 는 그리드 서비스를 이용하기 위한 대칭키를 GAMA 서버 내부적으로 생성하여, 포털의 사용자 계정으로 이용 가능하게 해줄 뿐 아니라 개발자에게 대칭키 발급을 위한 인증서버 및 대칭키의 관리, 대칭키를 이용한 로그인 시스템의 개발 부담을 덜어주는 장점이 있다.

MGrid 시스템의 나머지 요구사항들인 "서비스 계층에서의 사용자 식별", "웹 어플리케이션 사용자 인증", "포털과 웹 어플리케이션사이의 통합인증", "웹 어플리케이션 간 통합인증"은 포털과 웹 어플리케이션 간의 사용자 인증과 통합인증에 대한 것으로 사용자 계정 정보 내보내기, 가져오기 기능을 통해 포털 시스템 수준에서 통합인증을 수행하는 GAMA로 해결하기 어렵다. 또한 공개키와 개인키로 이루어진 대칭키를 기반으로 하는 보안메커니즘을 사용하는 그리드서비스계층에 LDAP, Kerberos와 같은 비즈니스 통합인증 솔루션을 적용하는 데는 많은 어려움이 있다.

3.3 UI 계층에서의 통합인증

통합인증은 포털과 포털, 포털 독립적인 웹 어플리케이션과 포털, 포털 독립적인 여러 웹 어플리케이션사이에서 가능하다. MGrid의 UI 계층에서는 이 3가지 경우 중 포털 독립적인 웹 어플리케이션과 포털, 포털 독립적인 여러 웹 어플리케이션사이의 통합인증을 위한 해결책이 필요하다. 따라서 이를 위한 통합인증 프로시저를 설계하고 그리드스피어 인증모듈과 JAAS 라이브러리를 통해 구현하였다.

3.3.1 JAAS 인증모듈

사용자가 작업 빌더(Job Builder)를 비롯하여 분석 및 시각화를 위한 웹 어플리케이션을 사용하려면 MGrid 포털에 로그인해야 한다. 이 때 사용자가 로그인한 정보를 통합인증에 사용하기 위해 JAAS[10]를 지원하는 그리드스피어 인증모듈을 작성하였다. JAAS는 자바에서 지원하는 플러그인 형태의 인증 프레임워크로 표준화된 메서드들을 제공할 뿐만 아니라 그 구현을 사용자환경에 맞게 수정할 수 있다. MGrid-security에 적용한 JAAS 인증 모듈은 사용자가 포털에 로그인 시 다음과 같은 일을 수행한다.

- 사용자의 계정 이름과 로컬 IP를 사용하여 UUID 형태의 임시 인증키 생성(auth-key)
- 생성된 인증키, 유효 기간, 사용자 계정 이름, 인증키로 암호화한 사용자 로컬 IP를 저장
- 웹 어플리케이션이 호출될 경우, 생성된 인증키를 인자로 받는다.

```
public class SimpleJAASLoginModule implements LoginModule {
    ...
    @override
    public void initialize(Subject subject,
                           CallbackHandler callbackHandler,
                           Map sharedState, Map options) {
        // initialize object properties
    }
    @override
    public boolean login() throws LoginException {
        Callback callbacks[] = new Callback[3];
        callbacks[0] = new NameCallback(...);      // Get login ID
        callbacks[1] = new PasswordCallback(...); // Get password
        callbacks[2] = new ClientIPCallback(...);  // Get Client IP
        callbackHandler.handle(callbacks);
        // retrieve login properties from callbacks
        ...
        return UserAuthManager.
                checkAuthenticate(username, password, userip);
    }
    ...
    @override
    public boolean logout() throws LoginException {
        // Retrieve login properties from callbacks.
        // See the login() method.
        ...
        return UserAuthManager.
                deleteUserAuthKey(username, password,userip);
    }
}
```

그림 2 JAAS 인증 모듈 의사 코드
Fig. 2 JAAS Login Module Pseudo Code

3.3.2 JAAS 인증 라이브러리

웹 어플리케이션이 인증할 수 있도록 구현한 라이브러리로 사용자 계정 이름과 포털 로그인 시 생성된 임시 인증키를 인자로 받는다. 구현된 JAAS 라이브러리는 다음 기능을 수행한다.

- 인증키를 사용하여 사용자의 로컬 IP와 인증키 생성시 암호화되어 저장된 로컬 IP를 비교한다.
- 포털에 로그인한 시간과 웹 어플리케이션 로그인한 시간을 비교하여 인증키의 유효기간을 검사한다.

3.3.3 통합인증 방안

사용자의 포털 로그인부터 웹 어플리케이션으로의 통합인증과정을 설명하면 다음과 같다. [그림4]

사용자가 포털에 로그인 정보인 계정 이름과 비밀번호를 전송하면 포털에서는 3.3.1절의 JAAS 인증 모듈에 인증을 위임한다. JAAS 인증 모듈은 3.3.2절의 라이브러리를 이용하여 1회용 인증키를 생성하여 저장한다. 포털에서 포털 어플리케이션이 아닌 일반 웹 어플리케이션으로 접근할 때, 포털은 인증된 계정과 발급된 1회용 인증키를 일반 웹 어플리케이션에 전달한다. 일반 웹 애플리케이션은 3.3.2절의 JAAS 라이브러리에 전달 받은 계정 이름과 1회용 인증키로 사용자의 인증 상태를 확인한 후, 다시 새로운 1회용 인증키를 생성해서 저장한다. 포털에 통합된 모든 웹 어플리케이션은 포털의 계정으로 인증된 상태로 접근해야 할 때마다, 새로운 1회용 인증키를 생성하고 기존에 발급된 1회용 인증키를 삭제함으로써 HTTP 프로토콜 상에서 평문으로 노출된 비밀번호 역할을 하는 인증키가 악의적으로 재사용되지 못하는 것을 보장한다

```
public class UserAuthManager {
    // Implemented by Single-ton design pattern
    public static String createUserAuthKey(String userID, userIP){
        UUID first = UUID.randomUUID();  // 32 char
        UUID second = UUID.randomUUID(); // 32 char
        ...
        String userAuthKey = first + second; // Remove char '-'.
        userAuthKey = insert(userID, userIP, currentTime,
                             userAuthKey, timeThreshold);
        // insert userAuthKey to repository
        // if repository has already userAuthKey,
        //     set userAuthKey to null value
        return userAuthKey;
    }
    public static String checkAuthentication(
                String userID, String userAuthKey, String userIP) {
        // Pseudo code
        storedUserID, storedUserIP = findBy(userAuthKey);
        return (storedUserID equal to userID) and
               (storedUserIP equal to userIP)
    }
    public static String deleteUserAuthKey(String userID, String
userAuthKey, String userIP) {
        // Pseudo code
        if( userIP is null ) {
            deleteBy(userID, userAuthKey);  // logout all clients
        } else {
            deleteBy(userID, userAuthKey, userIP);
                                    // logout only client@userIP
        }
    }
}
```

그림 3 사용자 인증 라이브러리
Fig. 3 User Authentication Library

IV. 평가

그리드 보안에 있어서 중요한 문제는 크게 6가지로 분류할 수 있다. 11)12)

1) 계정 관리 (account management)

인증과 허가에 앞서 그리드환경의 사용자를 식별하는 수단이 필요하며, 이를 위해 사용자 계정이 관리되어야 한다.

2) 인증 (authentication)

인증이란 그리드 서비스를 사용할 때 사용요청을 한 주체가 누구인지 확인하는 과정이다. 그리드 환경에서는 서비스 소비자가 서비스 제공자가 될 수 있기 때문에 서비스 소비자와 제공자간의 신분증명인 상호인증(Mutual Authentication)이 중요하다.

3) 허가 (authorization)

허가란 인증된 사용자에 대해서 그리드 서비스를 이용할 적절한 권한이 있는지 판단하는 과정이다. 이 때 사용자가 누구인지에 따라 차별성을 두기 때문에 인증이 선행되어야 한다.

4) 통합 인증 (single sign on)

사용자들이 그리드 자원을 사용하려면 가장 먼저 사용자 인증을 거쳐야 한다. 이 때 서로 다른 각각의 자원에 대한 사용자 인증과정을 한 번의 인증으로 통합하는 것이 통합인증기능이다.

5) 위임 (delegation)

권한위임이란 사용자의 작업을 처리하는 도중에 그리드 자원이 사용자를 대신해 또 다른 그리드 자원에 대한 인증을 처리하는 기능이다.

6) 무결성 및 기밀성 (integrity&confidentiality)

무결성이란 서비스 제공자와 소비자 사이의 메시지가 비인가자에 의해 무단으로 변경, 삭제, 생성되는 것을 방지하여 정보의 정확성, 완전성이 보장되도록 하는 것이다. 기밀성이란 정보가 비인가자에게 유출되지 않도록 비인가자의 시스템 접근을 통제하는 것이다.

이러한 그리드 보안의 중요문제들과 2장에서 언급한 MGrid 시스템의 보안 요구사항에 따라 기존 관련연구들의 특징을 비교하였다. GAMA, PURSE, Grid- Auth[13], DOE[14] 모두 사용자 인터페이스를 포털로 제공한다는 점에서 MGrid 의 요구사항을 만족시킨다. 또한 포털에서 사용자 계정 이름과 패스워드를 발급하고 내부적으로 사설 대칭키를 생성하여 사용자 계정 이름과 1:1 사상시켜 관리한다는 점에서 GAMA, GridAuth, PURSE는 유사하다고 할 수 있다. 이러한 메커니즘은 사용자가 그리드 서비스를 이용하기 위한 별도의 대칭키를 소유하지 않아도 되는 편리성이 있다. 그리드 보안 측면에서 GAMA는 계정관리와 인증 및 허가가 그리드스피어로 기반으로 구현된 포털에서 이루어진다. GAMA 서버구성요소들인 CACL[15], MyProxy[16]는 그리드 포틀릿 형태의 사용자 인터페이스와 분리되어 웹서비스 형태로 제공된다. GAMA는 그리드스피어의 인증모듈 형태로 배포가 용이하고 웹 어플리케이션에 대한 사용자 인증을 지원하지만 포털 간의 사용자 계정 정보 내보내기, 가져오기 기능을 통한 포털 수준의 통합인증에 그치고 있다. 표 1은 GAMA의 특징을 정리한 것으로 계정관리 및 인증, 허가를 주로 다루고 있음을 알 수 있다.

그리드 보안과 관련한 주요 문제 중 위임과 무결성 및 기밀성은 대칭키 기반으로 동작하는 그리드 환경의 경우 X.509[17] 스펙에 따라 충족됨으로 비교 기준에서 제외하였다.

본 논문에서 그리드스피어 포틀릿 프레임워크를 기반에서 JAAS 표준 기반으로 개발한3.3.1, 3.3.2 절에서 설명된 JAAS 인증 라이브러리를 사용하여, 포털 어플리케이션과 포틀릿 프레임워크에 종속적이지 않은 웹 어플리케이션간의 계정 통합과 그리드 인증 토큰을 안전하게 전달할 수 있는 방안을 제안하였다.

이를 통해서, 포털의 콘텐츠 개발에 있어 프레임워크에 종속적이지 않아도 포틀릿과 쉽게 통합될 수 있게 하고, 나아가 그리드 서비스에 접근을 용이하게 하였다.

그리드 서비스를 이용하는데 필요한 대칭키 발급을 위한 인증서버 및 대칭키의 관리 시스템의 개발에 관한 제반사항을 해결하기 위해 GAMA 시스템을 적용시켰다.

서비스 계층에서는 사용자 인증 및 식별을 사용자 개인 대칭키로 할 수 있는데, 이 경우 CAS[18]와 연동이 가능하다. 이를 통해 보다 더 정교한 역할 기반의 허가가 가능해진다. 그러나 현재 GAMA에서 제공하는 개인 대칭키를 사용하거나, 개인 대칭키를 따로 발급 및 관리하기 위해서는 추가개발이 필요하다.

따라서 MGrid-security 에서는 2장 2절에서 기술한 요구사항에 만족하기에 충분한 정도로 호스트 간 인증을 하였고, 사용자 계정 이름으로 식별을 하였다. 표 2는 MGrid-security의 특징을 정리한 것으로써 음영부분으로 표시된 것은 MGrid-security의 요구사항에 맞게 추가로 개발한 부분이다.

기존 연구에서는 특정분야의 문제 해결을 위해 최적화된 패키지형태로 배포되는 경우가 많다. 이것은 기존 시스템과의 통합에 어려움의 원인이 된다. 본 논문에서는 표준화된 프로토콜과 인터페이스를 준수하여 통합인증 기능을 구현함으로써, 시스템의 유연성을 향상은 물론 기존 시스템과의 연동이 용이하도록 하였다. 19)

표 1. GAMA의 특징
Table. 1 Feature of GAMA

layers / Grid / Security Area	UI layer			
	portal (그리드 스피어)	포털 종속 web app	포털 독립 web app	stand alone app
account mgmt	GAMA 인증모듈	-	-	-
identification	포털ID	포털ID	N/A	포털ID
authentication	GAMA 인증모듈	GAMA client interface	N/A	GAMA client interface
authorization	사용자 role	사용자 role	N/A	N/A
SSO	GAMA 가져오기/ 내보내기	default	N/A	N/A

표 2. MGrid-security 의 특징
Table. 2 Feature of MGrid-security

layers / Grid / Security Area	UI layer				service layer
	portal (그리드 스피어)	포털 종속 web app	포털 독립 web app	stand alone app	
account mgmt	GAMA 인증 모듈		-	-	-
identification	포털ID	포털 ID	포털 ID	포털 ID	포털 ID
authentication	수정된 GAMA 인증모듈 (JAAS)	GAMA client inteface	JAAS 인증 lib	GAMA client inteface	호스트 인증
authorization	사용자 role	사용자 role	N/A	N/A	N/A
SSO	GAMA 가져오기/ 내보내기	default	제안 방안	N/A	N/A

V. 결론 및 향후 과제

그리드의 보안문제는 분산된 자원들을 네트워크로 연결함에 따라 네트워크 시스템 인증과 사용자 인증 시스템 모두 필요하다. 특히 그 공유 대상이 실험결과와 같은 중요한 데이터들이기 때문에 높은 보안 수준을 필요로 한다. 따라서 대칭키 기반의 그리드 시스템과 사용자 계정 기반의 포털의 통합에 관한 연구들이 활발하다. 그러나 포털 시스템 수준에서 통합 인증을 수행하는 기존의 연구들은 포틀릿 프레임워크에 따라 작성된 포틀릿 어플리케이션과 포틀릿 프레임워크 밖에서 개발된 웹 어플리케이션간의 계정 통합 및 그리드 인증 통합이 필요한 경우, 적용에 많은 어려움이 있다. 또한 LDAP, Kerberos와 같은 비즈니스 통합인증 솔루션들은 그리드 서비스의 사용에 필수적인 대칭키 기반 인증 토큰을 어플리케이션 간에 공유할 수 있는 해결책이 없어 바로 적용하기는 어렵다.

본 논문에서는 그리드스피어 기반의 포틀릿 프레임워크 환경에서 MGrid security에 관한 요구사항들을 해결하기 위해서 포털 계정과 그리드 인증 시스템을 통합한 GAMA 시스템을 기반으로 하고, 포틀릿 프레임워크 환경에 밖에 존재하는 웹 애플리케이션에서 포털의 의해 제공되는 인증 토큰, 즉, 포털 계정 정보 및 그리드 인증 토큰을 사용할 수 있도록 하기위해서 본 논문에서 제안한 방법을 적용하였다.

이 방안의 특징은 UI 계층에서 포털 계정을 기준으로 사용자 인증과 허가를 수행하고, 그리드스피어 인증 모듈과 JAAS 표준 라이브러리를 제공함으로써 UI 계층에서 포털과 포털 독립적인 웹 어플리케이션간의 통합인증이 가능해졌다. 포털 사이트 구축에 있어 웹 어플리케이션을 개발할 때에, 인증 및 권한 제어로 인해 포틀릿 프레임워크에 종속적으로 개발할 수밖에 없었다. 본 논문에서 제안한 방안은 웹 어플리케이션에서 포틀릿 프레임워크에서 제공하는 인증 및 권한 제어 모델을 JAAS 표준으로 전이시킨다. 따라서 웹 어플리케이션의 개발에서 보다 폭넓은 프레임워크를 선택할 수 있고, 개발 결과물을 포플릿 프레임워크에 쉽게 통합할 수 있다.

향후 과제로 서비스 계층에서의 허가와 관련하여 보다 더 정교한 접근제어가 필요할 수 있다. 이를 위해서 인증서비스를 추가적으로 구현하거나 Role-based 기반의 CAS를 적용할 수 있다. CAS를 적용하려면 사용자가 개인 대칭키를 소유해야한다. 서비스 계층에서 정교한 접근제어 외에 통합 인증 기능이 필요할 수 있다. 이는 X.509의 위임 관련한 구현으로 해결 할 수 있을 것이다.

참고문헌

〔1〕 Jason Novotny, Michael Russell, Oliver Wehrens: "GridSphere: a portal framework for building collaborations," Concurrency - Practice and Experience 16(5): 503-513, 2004.

〔2〕 M.Russell,."GridPortlets overview," February 2005. *http://www.gridsphere.org/gridsphere/html/mardigrasworkshop2005/02 gridportlets.pdf*

〔3〕 OpenGrid Computing Environments Collaboratory, *http://www.ogce.org/, cited in May 2005.*

〔4〕 Thomas,M, et al. "The Gridport Toolkit: a System forBuilding Grid Portals," in 10th IEEE International Symp. on High Perf. Comp. 2001.

〔5〕 Karan Bhatia, Kurt Mueller, Sandeep Chandra, "GAMA: Grid Account Management Architecture," IEEE International Conference on EScience and Grid Computing, Dec. 2005

〔6〕 GridCenter, N., "A Portal-based User Registration Service for Grids," Apr. 2005. *http://www.gridscenter.org/solutions/purse/*

〔7〕 정갑주, 이종현, 조금원, 정선호, 황선태, 허대영, 최영진, "MGrid: 분자 시뮬레이션 그리드 시스템," 한국정보과학회, 정보과학회 학술발표논문집, 제 33권, 제 7호, 380-389쪽,1229-683X, 2006년 7월.

〔8〕 이종현, 김동욱, 이건영, 정갑주, 황선태, 박형우 "MGird Potal : 분자 시뮬레이션 그리드 포털," 한국정보과학회, 정보과학회 학술발표논문집. 제 31권, 제 1호, 457-459쪽, 1598-5164, 2004년 4월.

〔9〕 Youngjin Choi, Kum Won Cho, Karpjoo Jeong, Seunho Jung, "Molecular dynamics simulations of trehalose as a 'dynamic reducer' for solvent water molecules in the hydration shell. Carbohydrate Research," Elesvier Ltd, Vol. 341, pp.1020-1028, 0008-6215, Jun. 2006.

〔10〕 Java Authentication and Authorization Service, *http://java.sun.com/products/jaas/*

〔11〕 I. Foster et al., "Security Architecture for Computational Grids," ACM Conf. Computers and Security, ACM Press, New York, 1998.

〔12〕 이성현, 이재승, 문기영, "Research Trends of Grid Security Technology Based on Web Services," 전자통신동향분석 제 22권, 제 1호, 2007년 2월.

〔13〕 Timothy Warnock, Wei Deng, Lawrence Miller, Adam Lathers, "The GridAuth Credential Management System," 2005.

〔14〕 Burruss, J.R., Fredian, T.W., Thompson, M.R., "Simplifying FusionGrid Security," Challenges of Large Applications in Distributed Environments (CLADE) workshop at HPDC14, July 2005.

〔15〕 Link, W., "CACL, A CA System with Automated User Authentication," San Diego Supercomputer Center, Sept. 2003.

〔16〕 Novotny J, Tuecke S, Welch V. "An online credential repository for the grid: MyProxy," Proceedings of the 10th International Symposium on High Performance Distributed Computing IEEE Press: San Francisco, Aug. 2001.

〔17〕 Housley, R., Polk, W., Ford, W., and Solo, D., "X-509 Ceritficate" Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, IETF, Apr. 2002.

〔18〕 Pearlman, L., et al. "A Community Authorization Service for Group Collaboration," in IEEE 3rd International Workshop on Policies for Distributed Systems and Networks. 2002.

〔19〕 Ian Foster, Carl Kesselman, Steven Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International J. Supercomputer Applications, 15(3), 2001.

저 자 소 개

허 대 영

2004년 국민대학교 컴퓨터학부(학사)
2005년 국민대학교 전산과학(석사)
2006년 ~ 국민대학교 전산과학 박사 과정
관심분야 : e-Science, 그리드 시스템, PSE, 디자인패턴, 공개소프트웨어

황 대 복

2005년 국민대학교 컴퓨터학부(학사)
2006년 국민대학교 전산과학(석사)
2007년 ~ NHN
관심분야 : 그리드 시스템, 디자인패턴, 임베디드, 시스템아키텍쳐

황 선 태

1985년 서울대학교 컴퓨터공학과(학사)
1987년 서울대학교 컴퓨터공학과(석사)
1996년 Manchester University (Ph.D.)
1997년 ~ 국민대학교 전자정보통신대학 컴퓨터공학부 교수
관심분야 : e-Science, 그리드 시스템, PSE, 공개소프트웨어