매쉬업 서비스를 위한 OAuth 매커니즘 기반 사용자 통합 인증 플랫폼 개발

이다은○, 문승일, 홍충선*
daeunlee@khu.ac.kr, moons85@khu.ac.kr, cshong@khu.ac.kr
경희대학교 컴퓨터공학과

Development of Single Sign-On Platform Based OAuth Mechanism for Mashup Services

Da-Eun Lee○, Seung Il Moon, Choong Seon Hong*
Department of Computer Science and Engineering KyungHee University

요 약

현재 서로 다른 플랫폼을 연계한 다양한 매쉬업 서비스들을 제공되고 있다. 하지만 사용자가 이러한 매쉬업 서비스를 이용하기 위해서는 서비스마다 다르게 인증을 받아야 한다. 따라서 본 논문에서는 다양한 플랫폼을 연계해 주는 Smart Mediator와 매쉬업 서비스를 연동한 OAuth 기반의 통합 인증 구조를 제안했다. 이를 통해 각각의 매쉬업 서비스 개발자가 새로운 매쉬업 서비스 개발 시 사용자 인증 기술을 쉽게 적용 할 수 있는 효과를 기대한다.

1. 서 론

최근 Google API, Twitter API, Facebook API와 같은 Open API를 이용한 다양한 매쉬업 서비스가 제공 되고 있다[1]. 이 외에도 정부3.0 포탈 정보 등의 공공 데이터를 활용한 매쉬업 서비스들도 다수 등장하고 있다. 이러한 매쉬업 서비스들의 사용자 인증은 매쉬업 서비스마다 다르다. 이렇게 때문에 사용자는 매쉬업 서비스를 이용할 때 각각의 서비스에 맞는 인증을 해야 된다. 또한 매쉬업 서비스 개발자는 개별적으로 서비스에 대한 인증 서비스를 개발하여야 된다.

이렇게 때문에 매쉬업 서비스의 인증 서비스를 쉽고 편리하게 개발할 수 있는 Smart Mediator(SM)와 매쉬업 서비스를 연동한 통합 인증 구조가 필요 하다. 따라서 본 논문에서는 Open Authentication (OAuth) 매커니즘을 기반으로 하는 SM과 매쉬업 서비스 간의 사용자 통합 인증을 통해 사용자 인증을 용이하게 하는 연구를 진행하였다.[1)]

본 논문은 2장에서 제안하는 통합인증에 기반이 되는 OAuth에 대해 설명하고 3장에서는 매쉬업 서비스 통합 인증의 구조 및 실행 결과에 대해 설명한다. 4장에서는 타 서비스와의 기능을 평가한다. 끝으로 5장에서는 결론에 대해 논의한다.

이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R0126-15-1009, ICBMS 플랫폼 간 정보 모델 연동 및 서비스 매쉬업을 위한 스마트 중재 기술 개발)

*Dr. CS Hong is the corresponding author

2. 관련연구

2.1. Open Authentication

그림 1에서 볼 수 있듯이 Open Authentication (OAuth)는 서비스 소비자와 서비스 공급자 사이에서 토큰을 주고 받으며 사용자를 인증하는 표준 방법을 말한다[2].

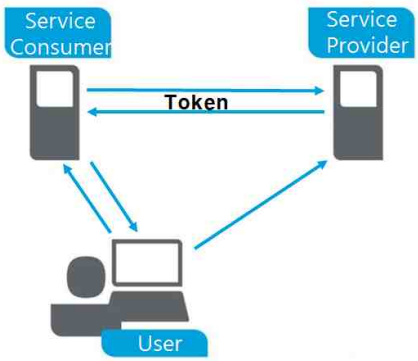

그림 1 OAuth 개념도

그림 2는 OAuth의 흐름도를 나타낸다. 그림 2에서 볼 수 있듯 이 OAuth는 서비스 공급자, 서비스 소비자, 사

용자 세 부분으로 나눌 수 있다[3].

사용자가 서비스 소비자의 서비스 이용을 요청하면 서비스 소비자는 서비스 제공자에게 Request Token을 요청하여 전송 받는다. Request Token을 받은 서비스 소비자는 사용자를 서비스 제공자의 로그인 페이지로 리다이렉트 한다. 사용자는 서비스 제공자의 로그인페이지에서 로그인을 한다. 사용자가 로그인을 하면 서비스 제공자는 서비스 소비자에게 사용자 인증 확인을 해주고 서비스 소비자는 서비스 제공자에게 Access Token을 요청하고 서비스 제공자를 이를 제공한다.

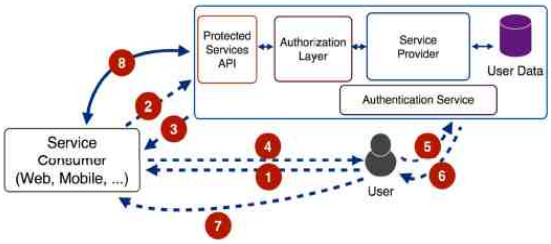

그림 3 OAuth 흐름도

3. 매쉬업 서비스 통합 인증

3.1. 구조

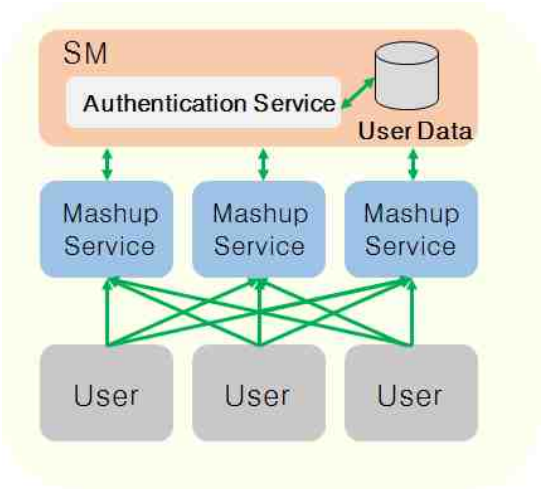

그림 4 매쉬업 서비스 통합 인증 구조도

본 논문에서 제안하는 OAuth를 기반으로 하는 매쉬업 서비스 사용자 통합 인증은 SM 계정으로 매쉬업 서비스가 사용자 인증을 할 수 있도록 하는 것을 목적으로 한다. 이를 위해 그림 3에는 매쉬업 서비스 통합 인증 구조를 도식화 하고 그림 4에는 매쉬업 서비스 통합 인증 절차를 시퀀스 다이어그램으로 나타내었다.

사용자가 매쉬업 서비스 사용 시 사용자 인증을 위해 로그인을 요청 하면 매쉬업 서비스는 SM에 Request Token을 요청한다. SM은 매쉬업 서비스에 Request Token을 전달하고 매쉬업 서비스는 SM의 로그인 페이

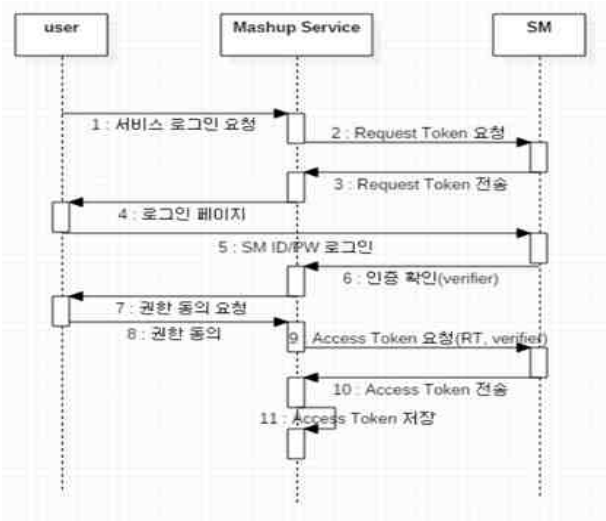

그림 2 매쉬업 서비스 통합 인증 시퀀스 다이어그램

지로 리다이렉트 한다. 사용자가 SM 계정으로 로그인하면 SM은 매쉬업 서비스에 Verifier 값을 전달한다. 매쉬업 서비스는 사용자에게 매쉬업 서비스가 SM에서 사용자 정보를 사용할 수 있도록 권한 동의를 요청하고 사용자는 권한을 동의한다. 이 과정이 끝나면 매쉬업 서비스는 Request Token과 Verifier 값을 가지고 SM에 Access Token을 요청한다. Access Token을 요청받은 SM은 매쉬업 서비스에 Access Token을 부여하고 매쉬업 서비스는 Access Token을 저장한다. 매쉬업 서비스는 사용자가 로그아웃을 하기 전까지 이 Access Token을 이용해 SM에 접근하여 사용자 정보를 이용 할 수 있다.

3.2. 개발 환경

Language	Java
DataBase	mysql
Persistence Framework	iBATIS2.0
Application Framework	Spring Maven
server	Tomcat 7.0

표 1 개발 환경

표1은 본 논문에서 구현한 사용자 통합 인증 플랫폼 서비스의 개발환경을 나타낸다.

3.3. 구현 결과

그림 5는 SM에 등록 된 매쉬업 서비스 정보를 나타낸다. 매쉬업 서비스가 생성되면 매쉬업 서비스는 자신의 정보를 SM에 등록한다. SM은 등록 된 매쉬업 서비스에게만 Request Token을 발급하도록 하였다.

매쉬업 서비스가 SM으로부터 Request Token을 발급받은 후 SM 로그인 페이지로 리다이렉트한 화면을 나타낸다. SM 로그인 페이지에서 로그인을 통해 사용자 인증을 한다.

그림 5 매쉬업 서비스 정보

그림 6은 사용자 인증 후 매쉬업 서비스에게 사용자 정보를 이용할 수 있는 권한을 부여할지 사용자의 동의를 얻는 과정이다. 권한 승인이 이루어지면 매쉬업 서비스는 Request Token과 Verifier 값으로 SM에 Access Token을 요청한다. SM은 매쉬업 서비스에 Access Token을 발급하고 사용자 인증과정을 끝낸다.

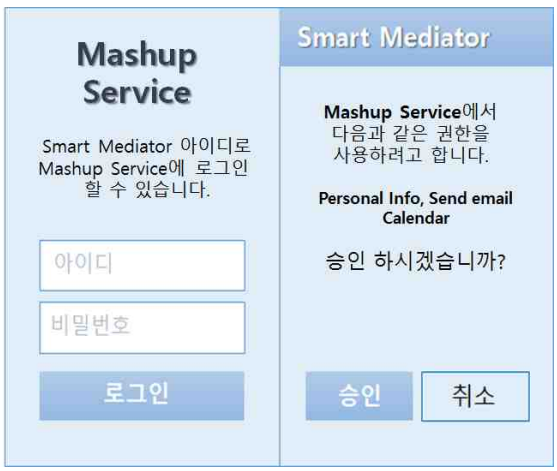

그림 6 로그인 및 권한 승인 페이지

4. 성능분석

Parameters	Value	
	www.mashup..or.kr	Smart Mediator
인증 API 제공	no	yes
인증 계정	n	1

표 2 타 서비스와의 비교표

표 2은 www.mashup.or.kr에서 제공하는 매쉬업 서비스와 본 논문에서 제안하는 매쉬업 서비스 인증 파라미터를 비교한 표이다.

SM은 자체 내에서 인증 API를 제공하는 반면에 www.mashup.or.kr은 자체 인증 API를 제공하지 않는다. 따라서 매쉬업 개발자는 google, Twitter와 같은 인증 API를 제공하는 서비스 제공자에게 개별적으로 인증키를 받아 인증 서비스를 제공하거나 자체 인증서비스를 구현해야 한다. 또한 사용자는 www.mashup.or.kr에서 제공하는 매쉬업 서비스를 사용 할 때 마다 각각 서비스에 맞는 인증 계정을 가지고 있어야한다. 하지만 본 논문에서 제안하는 SM 인증 방법은 SM에서 제공하는 API를 이용하기 때문에 사용자는 SM 계정으로 모든 매쉬업 서비스를 사용할 수 있고 매쉬업 개발자는 SM 인증 API로 사용자에게 인증 서비스를 쉽게 제공할 수 있다.

5. 결론

기존의 매쉬업 서비스 사용자 통합 인증은 Google, Twitter, Facebook 등에서 제공하는 API를 사용하여 매쉬업 서비스마다 제 각각의 인증 서비스를 제공하였다. 하지만 SM에서 매쉬업 서비스의 사용자 통합 인증 서비스를 제공함으로써 매쉬업 서비스 개발자는 매쉬업 서비스 개발 시 사용자 인증 기능을 쉽게 적용 시킬 수 있고 사용자는 SM 계정으로 다양한 매쉬업 서비스를 편리하게 이용할 수 있는 효과를 기대할 수 있다.

6. 참고문헌

[1] “Mashup(OpenAPI/Mashup)” 스마트 개발자 협회, http://www.mashup.or.kr/business/main/main.do

[2] D. Hardt, Ed, “The Oauth 2.0 Authorization Framework” , Microsoft, 2012

[3] Simone Cirani, Marco Picone, Pietro Gonizzi, Luca Veltri, Gianluigi Frerrai, “IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios” , IEEE Sensors Journal, vol. 15, Issue No. 2, pp1224-1234, Feb 2015

[4] Barry Leiba, “OAuth Web Authorization Protocol” , IEEE Internet Computing, vol.16 Issue No. 01, pp74-77, Feb 2012

[5] Ding Chu, Qing Liao, Jingling Zhao, “ Open Identity Management Framework for Mashup” , IEEE 2nd Symposium on Wob Society, pp378-382, Aug 2010