공개된 서로 다른 보안 플랫폼들을 통합하기 위한 보안 어댑터 설계

김성수○ 홍충선*
경희대학교 컴퓨터공학과
{ mjs0514, cshong }@khu.ac.kr

Design of Security Adaptor to integrate Different Open Security Platforms

Sung Soo Kim○ Choong Seon Hong*
Department of Computer Engineering, KyungHee University

요 약

현재 IT 트렌드로 이슈된 여러 기술들이 서로 연계되어 다양한 매쉬업 서비스들을 제공하고 있다. 하지만 여러 기술들을 연계함에 따라 여러 보안 이슈들도 발생하게 된다. 이를 해결하기 위해 이종의 보안 플랫폼들을 통합한 보안 어댑터를 설계했다. 이를 통해 새로운 매쉬업 서비스의 개발 시 보안 기술을 쉽게 적용할 수 있는 효과를 기대할 수 있다.

1. 서 론

2015년 투비소프트는 국내 IT업계에 종사하는 자사 고객을 대상으로 한 설문조사에서 현재 IT 트렌드로 IoT와 빅 데이터를 꼽았다고 발표했다.[1] 그 외에도 미래인터넷 산업으로 여전히 주목받고 있는 클라우드와 같은 기술들이 있다. 중요한 점으로는 이와 같은 각각의 기술들이 이제는 더 이상 개별적으로만 사용되지 않는 다는 것이다. 그 사례로 구글을 살펴보면 여러 기술들을 접목한 매쉬업 서비스들을 제공하는 것을 볼 수 있다. 이러한 서비스 동향들을 살펴보고 이에 따라 다양한 기술들을 연계한 매쉬업 서비스 개발과 관련된 연구를 해야 한다.

하지만 이 연구를 위해서 우선적으로 해결해야할 문제가 있다. 다양한 기술들을 연계 하게 되면 그에 따라 보안 문제가 발생할 수밖에 없다. 예를 들면 클라우드 상의 데이터를 가지고 빅 데이터 분석을 위한 매쉬업 서비스에서는 데이터의 익명화나 클라우드 상에서 발생하는 로그들을 모니터링 하는 등의 보안기술들이 필요할 것이다. 이와 같이 매쉬업 서비스가 제공하는 기능들에 따라 맞는 보안 매쉬업 서비스를 제공해야 한다. 그러기 위해서는 서로 다른 보안 플랫폼들을 통합해서 제공하는 어댑터가 필요하다. 본 논문에서는 이 어댑터를 통해 보안 매쉬업 서비스 개발을 용이하게 하는 연구를 진행했다.

본 논문의 구성은 다음과 같다. 2장에서 보안 어댑터(Security Adaptor)를 구성요소로 가지는 SM(Smart Mediator)에 대해서 설명하고 3장에서 제안하는 보안 어댑터의 기능과 구조를 설명한다. 그 후 끝으로 결론 및 향후 연구 계획에 대하여 논한다.

본 연구는 미래창조과학부 및 정보통신기술 진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [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. Smart Mediator [2][3]

2.1 개요

Smart Mediator란 그림 1에서 볼 수 있듯이 클라우드 내부에서 IoT, 빅 데이터, 클라우드 등과 같은 기술들의 플랫폼들을 연계해서 새로운 매쉬업 서비스를 개발할 수 있도록 제공하는 환경을 말한다.

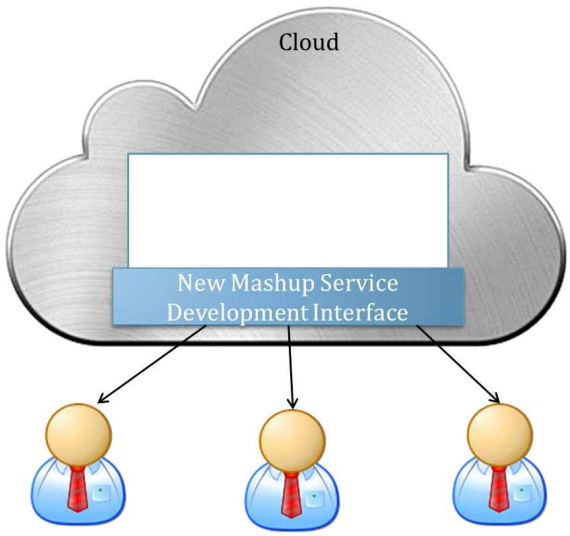

그림 1. Smart Mediator

2.2 구조

그림 2는 SM 내부에서 보안 어댑터와 관련이 있는 부분만을 나타낸다. 이것은 각각 어댑터 계층, 서비스 계층, 개발 계층으로 나눌 수 있다.

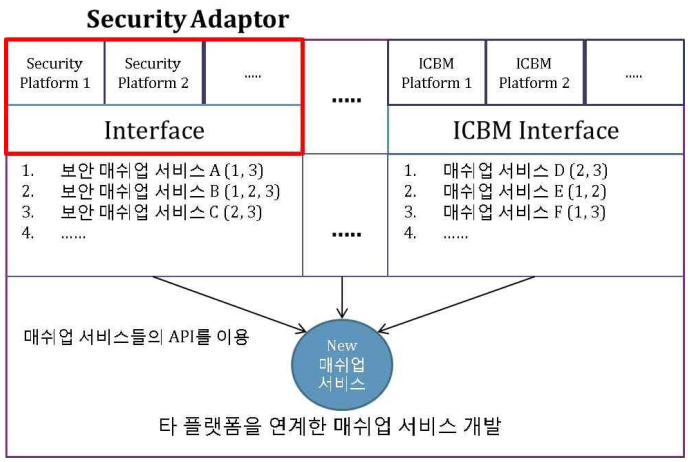

그림 2. SM의 내부에서 Security Adaptor의 역할

먼저 어댑터 계층은 IoT, Cloud, Big Data, Mobile의 기술들이 가지는 다양한 오픈 플랫폼들을 하나로 통합한 어댑터들의 그룹이다. 본 논문에서는 이 계층의 보안 어댑터만 설계한다. 두 번째로 서비스 계층은 어댑터 내부에 있는 플랫폼만 가지고 만든 매쉬업 서비스들을 등록한 계층이다. 마지막으로 개발 계층은 서로 다른 어댑터의 플랫폼들과 연계하여 새로운 매쉬업 서비스를 개발할 수 있도록 하는 계층이다.

서비스 계층을 자세히 보면 각각 다른 조합으로 만들어진 A, B, C 라는 보안 매쉬업 서비스가 등록되어 있는 것을 볼 수 있다. 사용자는 새로운 매쉬업 서비스를 개발할 때 미리 등록된 매쉬업 서비스들의 API를 통해 원하는 기능을 구현할 수 있다.

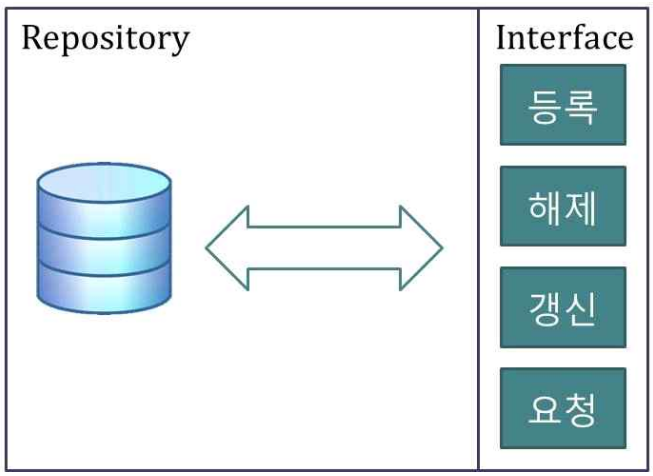

그림 3. 보안 어댑터의 기능 정의

3. 보안 어댑터(Security Adaptor)

본 논문에서 제안하는 보안 어댑터는 여러 가지 공개된 보안 플랫폼들을 하나의 어댑터로 통합해서 보안 매쉬업 서비스를 만들 때 원하는 플랫폼의 기능을 쉽게 제공하는 것을 목적으로 한다. 이를 위해 그림 3에 보안 어댑터에 필요한 기능을 도식화 했다. 첫 째로 보안 어댑터 내부의 저장소에 새로운 플랫폼을 등록하는 기능이 필요하다. 두 번째는 반대로 사용하지 않는 플랫폼을 해제하는 기능이 필요하다. 세 번째로 등록된 플랫폼을 수정할 수 있는 기능도 필요하다. 마지막으로 사용자가 보안 어댑터에게 사용하고자 하는 플랫폼을 요청하는 기능이 필요한데, 이는 그림 4를 통해 프로세스를 나타냈다.

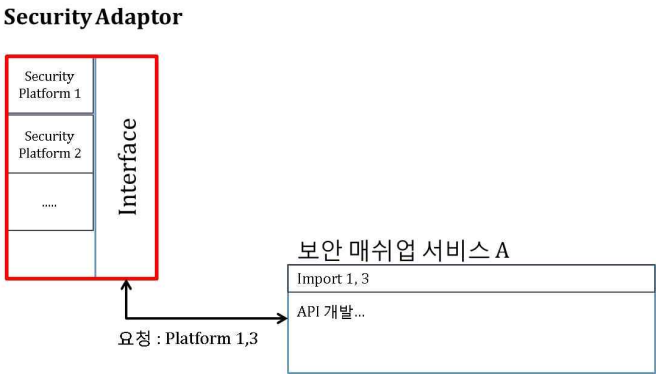

그림 4. 요청 프로세스

4. 결론 및 향후 연구 계획

이미 서로 다른 플랫폼들을 연계해서 시너지 효과를 내는 서비스들이 나타났으며 앞으로도 그 시장이 커질 것으로 보인다. 그러므로 보안 어댑터를 통해 새로운 매쉬업 서비스의 개발 시 보안 기술을 쉽게 적용할 수 있는 효과를 기대할 수 있다.

향후 연구 계획으로는 보안 어댑터를 구현해서 성능 평가를 위한 기준을 정의하고 얼마만큼 쉬운 개발 환경을 제공하는지 비교 분석을 할 계획이다.

5. 참고문헌

[1] 팽동현, “국내 IT업계 화두, ‘IoT’와 ‘빅데이터’”, IT DAILY, 2015, http://www.itdaily.kr/news/articleView.html?idxno=62832

[2] J. Im, S. Kim, and D. Kim, “IoT Mashup as a Service: Cloud-based Mashup Service for the Internet of Things,” in Proc. 10th International Conference on Services Computing (SCC), pp. 462-469, June, 2013.

[3] 이용주, “Open API를 활용한 클라우드 기반 모바일 매쉬업 개발”, 한국정보기술학회논문지, 제12권, 제3호, pp. 155-161, March, 2014.