클라우드를 위한 통합 인증 관리 시스템에 적용 가능한 오픈 소스 조사 및 평가

*최영락, **리건, **정태열, *홍원기
*포항공과대학교 정보전자융합공학부, **포항공과대학교 컴퓨터공학과
{dkby, gunine, dreamerty, jwkhong}@postech.ac.kr

Survey and Evaluation of Open Sources for Integrated Authentication Management System in Cloud Infrastructure

*Yeongrak Choi, **Jian Li, **Taeyeol Jung and *James Won-Ki Hong
*Division of IT Convergence Engineering, POSTECH,
**Department of Computer Science and Engineering, POSTECH.

요 약

현재 클라우드 컴퓨팅에서 보안 문제는 클라우드 컴퓨팅 도입 및 활성화를 위해 가장 먼저 해결되어야 할 과제로 인식되고 있다. 클라우드 컴퓨팅 보안 요구 사항 중 가장 대표적인 사항은 다양한 장치들로부터의 통합 인증을 안전하게 수행하는 것이다. 본 논문에서는 클라우드를 위한 통합 인증 관리 시스템에 적용 가능한 오픈 소스들을 알아보고, 조사된 오픈 소스들을 평가하여 해당 오픈 소스를 시스템 구축에 적용할 때, 개발 시간 및 비용 절감 등의 오픈 소스의 이점을 활용하는 데 도움을 주고자 한다. 시스템 구축에 적용시 고려해야 할 편의성, 수정 및 확장 용이성, 라이선스를 주요 평가 기준으로 하여 관련 오픈 소스들을 평가하였다.

Ⅰ. 서 론

현재 클라우드 보안 문제는 클라우드 서비스 도입을 위해 가장 먼저 해결되어야 할 문제로 인식되고 있다. IDC 가 2008 년 발표한 자료 [1]에 따르면, 클라우드 서비스 도입과 관련해 가장 중요하게 생각하는 이슈로 응답자의 74.6%가 보안이라고 답했다. 뿐만 아니라 최근 몇몇 대형 업체에서 발생한 클라우드 보안 사고들 [2][3]은 클라우드 서비스의 신뢰와 투명성 확보를 어렵게 하고 있다. 클라우드 컴퓨팅 보안 문제를 해결하기 위한 다양한 보안 요구 사항들이 제기되고 있다 [4]. 특히 다양한 이기종의 장비들을 통해 여러 장소에서 클라우드 인프라에 인증 및 접근을 통해 이루어지는 클라우드 서비스의 보안을 대비하기 위해서는 안전한 인증 및 Identity 관리를 위한 통합 인증 관리 시스템의 도입이 필요하다.

클라우드를 위한 통합 인증 관리 시스템을 구현하는 방안 가운데, 오픈 소스 소프트웨어를 활용한 개발은 다양한 요구 사항에 유연하게 대응이 가능하고, 제반 비용을 절감할 수 있다는 장점이 있다 [5]. 본 연구는 클라우드를 위한 통합 인증 관리 시스템을 구현할 때 적용 가능한 오픈 소스들을 조사 및 분석하는 것을 목표로 한다. 오픈 소스들을 선정하여 평가함에 있어서 시스템 구축에 적용시 편의성, 소스 수정 및 확장 용이성, 라이선스 관련 요소들을 중점적으로 클라우드 통합 인증 관리 시스템을 구축할 때 고려해야 할 사항들을 살펴볼 수 있을 것이다.

Ⅱ. 본 론

본 장에서는 클라우드를 위한 통합 인증 관리 시스템의 개요에 대해 설명하고, 이에 적용 가능한 오픈 소스들의 조사 및 평가 결과를 보인다.

1. 클라우드를 위한 통합 인증 관리 시스템 개요

클라우드에 접근하는 서비스 사용자들은 다양한 IT 자원을 통하여 클라우드에 접속하여 클라우드에서 제공하는 서비스를 이용한다. 악의적인 사용자가 타인을 사칭하여 클라우드에 접속하여 사용한다면, 클라우드 내 해당 사용자에 대한 모든 데이터 접근 및 리소스 사용이 이루어지고 이에 따른 과금 유발 등과 같은 보안 사고가 발생할 수 있다. 따라서 보안성이 강화된 통합 인증 관리 시스템이 필요하다. 해당 시스템은 클라우드에 접속하는 사용자 신원 확인, 인증 과정, 인증 단말 목록 관리, 인증을 수행하기 위한 안전한 통신 채널 관리, 인증 세션 관리 등과 같은 인증과 관련된 전반적인 기능을 담당한다.

2. 적용 가능한 오픈 소스 조사

본 연구는 한국연구재단을 통해 교육과학기술부의 세계수준의 연구중심대학육성사업(WCU)으로부터의 지원받아 수행 (R31-2010-000- 10100-0) 및 방송통신위원회의 "HiMang (Highly Manageable Network and Service Architecture for New Generation) 원천 연구" 원천기술개발사업의 연구결과로 수행 (KCA-2011-10921-05003) 되었습니다.

클라우드를 위한 통합 인증 관리 시스템에 적용 가능한 오픈 소스로 다음과 같은 오픈 소스들을 선정하여 조사하였다. 괄호는 라이선스 종류를 나타낸다.

- WSO2 Identity Server (License: Apache v2)
  오픈 소스 기반의 신원 및 자격을 관리하는 시스템으로, XCAML 2.0 에 의한 자격 관리 엔진을 포함하고 있으며, 요청 기반의 보안 토큰 서비스, OpenID 제공, Information Card 규격 지원, 사용자 요청 관리 등의 다양한 관리적인 기능을 지원한다.
- Kerberos (License: MIT)
  네트워크 인증 프로토콜 중 하나인 Kerberos 에 대해 대해 MIT 에서 구현한 것을 오픈 소스화한 버전이다.
- OpenLDAP (License: 자체 규정 라이선스)
  LDAP 프로토콜에 대한 오픈 소스 구현 버전이다.
- OpenSSL (License: 듀얼 라이선스로 규정)
  네트워크를 통한 데이터 통신에 쓰이는 프로토콜인 TLS 와 SSL 를 구현한 오픈 소스이다. C 언어로 작성되어 있는 중심 라이브러리 안에는, 기본적인 암호화 기능 및 여러 유틸리티 함수들이 구현되어 있다.
- OpenSSH (License: BSD)
  SSH (Secure SHell) 프로토콜을 구현한 오픈 소스로, 기존의 안전하지 않은 telnet, ftp, rlogin, rsh, rcp 와 동일한 기능을 수행하는 안전한 도구들을 제공하며, 터널링 등을 통해 클라이언트와 서버와의 통신, 각 머신으로의 원격 접속시 안전한 접속을 위한 통신 채널을 제공한다.
- OpenPAM (License: New and Simplified BSD)
  BSD 계열 운영체제 (FreeBSD, NetBSD), Mac OS X 에서 또는 몇몇 리눅스 배포판에서 Linux PAM 을 대체하여 사용하는 Pluggable Authentication Module (PAM)에 대한 오픈 소스이다.
- GnuPG (License: GNU GPL v3)
  통신상에서 혹은 데이터를 저장할 때 보안을 지키는 도구이다. 데이터를 암호화하고 전자 서명을 만들 수 있으며 암호화 도구로 Pretty Good Privacy (PGP) 기능을 제공한다.

3. 오픈 소스 평가 결과

표 1 과 표 2 는 실제 적용시 편의성, 수정 및 확장 용이성, 라이선스 평가에 대한 세부 기준 및 이들을 점수화한 평가 결과를 나타낸다. 실제 적용시 편의성은 오픈 소스를 도입하여 클라우드 통합 인증 시스템에 도입할 때 다운로드, 설치, 이식성, 문서화, 지원 여부를 고려하여 평가하였고, 수정 및 확장 용이성은 개발 언어 특성 및 소스의 모듈화 정도와 오픈 소스 제공자가 해당 오픈 소스를 주기적으로 유지 보수 하는지를 평가 항목으로 정하였다. 라이선스는 서비스 제공자가 도입시 고려해야 할 각 라이선스 종류에 따른 상업화 가능 여부 및 타 라이선스 호환성, 소스 공개 의무를 기준으로 평가하였다.

평가 결과 인증 관리 오픈 소스인 WSO2 Identity Server 가 전반적으로 우수함을 보였으며, GnuPG 의 경우 라이선스 부분에서는 수정 소스 공개 의무가 있어 낮은 점수를 보였다. 수정 및 확장 용이성을 평가하기 위해 사용한 오픈 소스 버전은 각각 WSO2 Identity Server 3.2.2, Kerberos 1.9.2, OpenLDAP 2.4.28, OpenSSL 1.0.0e, OpenSSH 5.9p1, OpenPAM Lycopsida, GnuPG 2.0.14 이다.

표 1. 오픈 소스 평가 - 실제 적용시 편의성

오픈 소스	실제 적용시 편의성				
	설치 편의성	설명 제공	이식성	문서화	기술 지원
WSO2 Identity Server	2.5	3.3	5	4.5	5
Kerberos	4.5	5	4.2	5	3
OpenLDAP	4.5	5	4.2	4.5	5
OpenSSL	4.5	5	4.2	3.5	5
OpenSSH	4	5	4.2	2.5	3
OpenPAM	4	5	3.3	1.5	1
GnuPG	2.5	5	5	4.5	3

표 2. 오픈 소스 평가 – 수정 및 확장 용이성, 라이선스

오픈 소스	수정 및 확장 용이성		라이선스			
	개발 소스 관련	코드 유지 보수	라이선스 종류	상업화	타 라이선스 호환성	소스 공개 의무
WSO2 Identity Server	2.9	5	Apache v2	Y	Y	N
Kerberos	2.3	5	MIT License	Y	Y	N
OpenLDAP	2.5	5	자체 규정	Y	Y	N
OpenSSL	1.8	2	듀얼 (OpenSSL Toolkit + SSLeay)	Y	Y	N
OpenSSH	2.3	2	BSD	Y	Y	N
OpenPAM	2.1	5	BSD	Y	Y	N
GnuPG	3.1	3.5	GNU GPL v3	N	N	Y

Ⅲ. 결 론

본 연구에서는 클라우드를 위한 인증 관리 시스템의 개요를 설명하고, 해당 시스템에 적용 가능한 오픈 소스를 선정하여 관련 오픈 소스들을 조사하고 실제 적용시 편의성, 수정 및 확장 용이성, 라이선스 기준에 따라 평가하였다. 본 연구 결과를 토대로, 실제 시스템 구현시 해당 오픈 소스의 기능을 활용해 효율적인 구현이 가능해질 것이다. 향후 연구로 해당 오픈 소스에 대한 기능 및 성능에 대한 평가 및 시스템 프레임워크 설계 등을 진행할 것이다.

참 고 문 헌

[1] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits & Challenges", IDC eXchange, Sep. 2008.

[2] V. P. Y. Chen, R. H. Katz, "What's New About Cloud Computing Security?", EECS Department, UC Berkeley, UCB/EECS-2010-5, Jan. 2010.

[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no 1, 2011, pp. 1-11.

[4] 이형효, "클라우드 컴퓨팅 보안 연구 동향", 정보통신산업진흥원 주간기술동향 1525 호, Dec. 2011, pp. 12-23.

[5] 박창근, 김기응, 유재형, "오픈 소스 소프트웨어 기반의 망 관리 시스템 개발", KNOM Review, vol. 13, no 1, Jul. 2010, pp. 46-54.