클라우드 컴퓨팅에서의 개인사용자를 위한 접근제어 시스템

박준영*, 나상호*, Yuan Tian*, 허의남*
*경희대학교 컴퓨터공학과
e-mail: jypark|shna|tianyuan@icns.khu.ac.kr, johnhuh@khu.ac.kr

A Access System for a Personal User in the Cloud Computing

Jun-Young Park*, Sang-Ho Na*, Tian Yuan*, Eui-Nam Huh*
*Dept of Computer Engineering, Kyung-Hee University

요 약

클라우드 컴퓨팅 서비스는 눈부신 발전으로 다양한 서비스가 제공되고 있으며 많은 개인 사용자들이 클라우드 서비스에 가입하여 서비스를 제공받고 있다. 하지만 개인 사용자를 대상으로 제공하는 클라우드 서비스는 사용자의 정보를 요구하고 있으며 제공된 사용자 개인정보가 어떻게 보고되는지 개인 사용자는 확인하기 힘들다. 따라서 사용자의 정보 공개를 최소화하는 시스템이 필요하며 사용자의 정보가 없어도 사용자에 맞춤 서비스를 제공할 수 있는 클라우드 컴퓨팅 접근제어 시스템을 제안하고자 한다.

1. 서론

클라우드 컴퓨팅 서비스가 활성됨에 따라 구글, 아마존, 애플, 마이크로 소프트와 같은 국외 IT대기업을 중심으로 국내에도 많은 클라우드 서비스가 제공되고 있다. 또한 클라우드 컴퓨팅 서비스가 모바일 단말기까지 서비스를 제공하면서 클라우드 컴퓨팅 서비스는 기업에서 개인 사용자로 서비스 대상이 변하였다.

하지만 클라우드 컴퓨팅 서비스가 개인 사용자에게로 확대되면서 많은 문제가 발생하고 있다. 클라우드 서비스 제공자는 개인 사용자에게 편리한 서비스를 제공하지만 사용자의 동의없이 무분별한 개인정보를 수집 등으로 인해 개인정보 보호에 대한 필요성이 부각되었다.

따라서 다양한 서비스의 결합이 제공되기 위해서는 개인정보 노출이 적으며 올바른 사용자 여부를 확인할 수 있는 명확한 인증절차가 수반되어야 한다.

본 논문에서는 2장에서 클라우드 컴퓨팅 서비스 모델, XACML, Azure 접근제어 서비스, RBAC에 대해서 알아본다. 그리고 3장에서는 클라우드 컴퓨팅에서의 접근제어 시스템을 제안 및 각 컴포넌트 정의하며 4장의 결론에서 본 논문의 요약과 향후 연구방향을 제시한다.

2. 관련연구

2.1. 클라우드 컴퓨팅 서비스 모델

클라우드 컴퓨팅 서비스 구조는 국제 표준화 기구인 ITU-T Focus Group on Cloud Computing(FG Cloud)에서 정의하고 있는 클라우드 컴퓨팅 서비스 모델을 기반으로 한다[1].

2010년도 2월 국제표준화 기관인 ITU-T에서 클라우드 컴퓨팅 기술 표준을 위한 FG Cloud 그룹을 구성하였으며 클라우드 컴퓨팅의 요구사항 및 Cloud Ecosystem 등을 정의하였다. 또한 다음과 같이 클라우드 컴퓨팅 서비스에 대한 3가지 도메인을 정의하였다[2].

- **End User Request and Access**

  최종 사용자들의 활용 용도에 맞는 서비스 품질과 보안 수준을 관리하며 클라우드 서비스 제공자와의 서비스 연결에 필요한 서비스를 포함

- **Provider Cloud Orchestration**

  기존의 IaaS, PaaS, SaaS 뿐만 아니라 서비스 제공자들 간의 서비스 연동을 통한 다양한 서비스모델 및 유스케이스 (Use-Case)를 제공

- **Virtualized Resource Management**

  IaaS, PaaS, SaaS와 같이 자원을 가상화하여 서비스 제공에 제한이 없도록 관리와 각 서비스를 사용자 임의로 이용이 가능하도록 제공

End User Request and Access는 사용자 입장에서 인트라넷과 같은 안전하고 편리한 환경 제공을 위함이며, Provider Cloud Orchestration을 통해 현재까지 알려진 서비스 모델 그 이상의 서비스 간 연동(Inter Cloud)을 고려하고 있다. 또한 서비스 제공자에 구애 받지 않을 수 있는 서비스 간 자원 연동을 위하여 Virtualized Resource Management를 제시하였다.

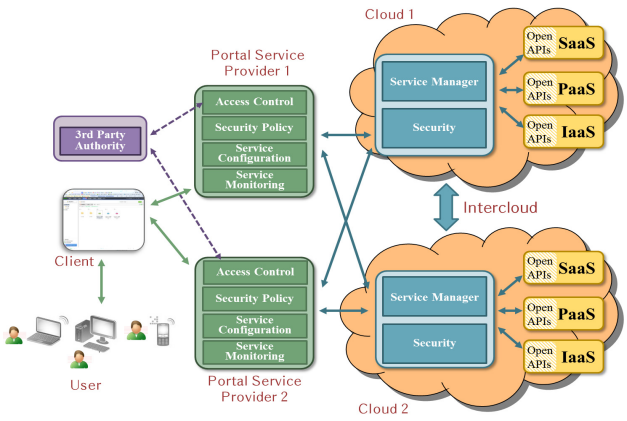

그림 1. 클라우드 컴퓨팅 서비스 참조 모델

그림 1과 같이 사용자는 Client를 이용하여 클라우드 컴퓨팅 서비스를 제공받을 수 있는데, 여러 서비스 제공자가 존재할 것이며, 제공자에 따라 서로 다른 서비스 제공과 서비스 정책이 존재할 것이다. 또한 제공자들간의 협력관계가 생성되어 제공자들간의 자원연동이 가능하고 사용자의 안정성과 편의성을 갖춘 컴퓨팅 환경이 제공될 수 있다. 이는 단일 클라우드 서비스 제공자에 종속되지 않고 클라우드 간(Inter Cloud) 연동 및 확장을 통해 폭넓은 서비스를 제공을 위함이다. 이러한 요구사항들을 충족하기 위해서는 클라우드 컴퓨팅 서비스 제공자와 다양한 서비스를 제공받고 싶은 사용자간에 Portal Service 혹은 Portal Service Provider가 존재하여 사용자가 원하는 서비스를 구성 및 제공한다. 서드파티(3rd Party) 인증으로 서로 다른 클라우드 서버의 서비스를 제한 없이 제공받을 수 있다.

또한, 클라우드 서버의 Service Manager는 서버내의 서비스 관리 및 User Profile에 따른 서비스를 관리한다. 클라우드 내 보안, 서비스 자원 감사 및 사용자 서비스 접근 제어는 Security컴포넌트에서 수행된다[1].

2.2. XACML(eXtensible Access Control Markup Language)

XACML이란 국제 표준화 단체인 OASIS에서 제정한 기술이며 국제 표준웹 환경 하에서 인증과 권한 정보 등의 보안 정보를 전달하기 위한 데이터 구조를 정의하는 표준이다. 접근제어는 요구된 자원 접근이 허용되어야 하는지에 대한 판단 정보와 접근 결정을 시행하기 위한 정보들로 구성되어 있다. 접근제어 정책은 접근제어 결정을 위한 기준이 된다. XACML 핵심 규격은 인가 정책을 평가하기 위한 문법과 규칙으로 정의되고 있다. XACML은 대규모 환경에서 동작하며 접근 제어용으로 이용되는 정보가 자동화된 주체에 의하여 관리되는 응용을 위해 효율적으로 동작되도록 설계되어 있다[6].

- **속성(Attribute):** 서브젝트(subject), 자원(resource), 액션(action) 또는 술어(predicate)나 목표(target)에서 참조를 하게 될 수 있는 환경의 특징
- **정책관리지점(PAP: Policy administration point):** 정책이나 정책집합을 생성하는 시스템 요소
- **정책결정점(PDP: Policy decision point):** 적용 가능한 정책을 평가하고, 권한부여 결정을 만드는 시스템 요소
- **정책시행점(PEP: Policy enforcement point):** 결정 요청을 생성하고, 권한부여 결정을 시행하여 접근제어를 수행하는 시스템 요소
- **정책정보지점(PIP: Policy information point):** 속성 값의 근원지 역할을 하는 시스템 요소

2.2.1. XACML 데이터 흐름 다이어그램

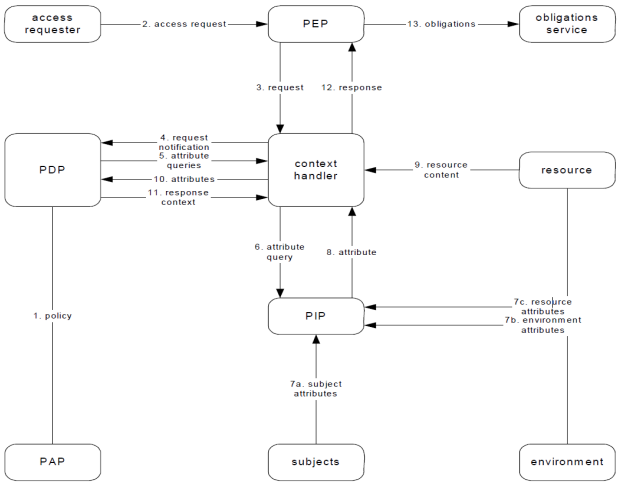

그림 2. XACML 데이터 흐름 다이어그램

XACML의 데이터 흐름은 다음 단계들에 따라 동작한다[4].

1. PAP들은 정책들과 정책집합들을 작성하여, PDP가 이용할 수 있도록 한다. 이러한 정책들과 정책집합들은 특정 목표에 대해 완전한 정책을 나타낸다.
2. 접근 요청자는 PEP에게 접근요청을 보낸다.
3. PEP는 원형식의(native request format)의 접근요청을 문맥처리기(context handler)에 보낸다. 이 접근 요청은 서브젝트, 자원, 액션과 환경의 속성들을 선택적으로 포함하고 있다.
4. 문맥 처리기는 XACML 요청 문맥을 생성하여, PDP에게 그것을 보낸다.
5. PDP는 문맥 처리기에 추가적으로 서브젝트, 자원, 액션, 환경 및 (그림에서 보여주진 않지만) 다른 카테고리 속성들을 요청한다.
6. 문맥 처리기는 속성들을 PIP에게 요청한다.
7. PIP는 요청된 속성들을 얻는다.
8. PIP는 요청된 속성들을 문맥 처리기에 반환한다.
9. 선택적으로, 문맥 처리기는 문맥에 자원들을 포함시킨다.
10. 문맥 처리기는 요청받은 속성들과 (선택사항)자원들을

PDP에게 보낸다. PDP는 정책을 평가한다.

11. PDP는 응답 문맥(권한부여 결정을 포함)를 문맥 처리기에 보낸다.
12. 문맥 처리기는 응답 문맥을 원형식의 PEP 응답 포맷으로 변경한다. 문맥 처리기는 그 원시응답을 PEP에게 반환한다.
13. PEP는 의무를 이행시킨다.
14. (그림에 나타나있지는 않지만) 만일 접근이 허가된다면, PEP는 자원에 대한 접근을 허가한다. 그렇지 않으면, PEP는 접근을 거부한다.

2.3. 애져 접근제어 서비스 (Azure Access Control Service)

애져 접근제어 서비스는 클라우드에서 표준기반의 토큰을 발행한다(호스트, 모든 앱패브릭(AppFabric)계정을 사용할 수 있는 멀티테넌트(Multi-tenant)). 닷넷(.NET) 접근제어 서비스는 인증 및 권한부여 서비스를 외부의 보안 전문가가 관리할 수 있게 제공한다. 애져의 보안 전문가들은 인증과 토큰 발행을 제어한다. 따라서, 어플리케이션은 인증절차를 토큰확인으로 대신한다[3].

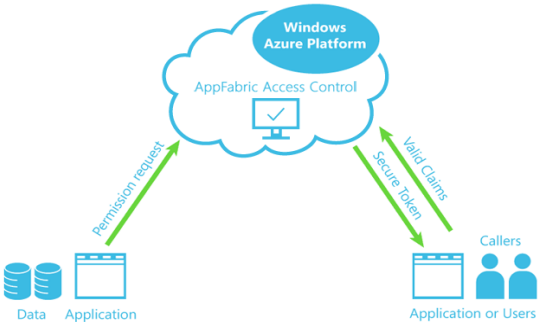

그림 3. Azure 접근제어 서비스 프레임워크

2.4. 역할기반 접근제어(RBAC)

역할기반 접근제어는 퍼스널 클라우드 접근제어를 연구하기 위한 기본 개념이 된다. 역할기반 접근제어는 조지매이슨 대학의 Ravi Sandhu에 의해 제안되었다. 1996년에는 특정 데이터 또는 리소스에 권한이 있는 사용자만 접근이 가능하였다.

오늘날, 역할기반 접근제어(RBAC) 모델은 헬스케어 분야에서 널리 사용되고 있다. 왜냐하면 일반적인 병원은 (환자, 의사, 간호사 등) 역할을 확실하게 구분이 되어있다.

현재의 역할기반 접근제어 시스템은 그림 4와 같다. 사용자의 역할에 따라 권한 부여는 시스템 관리자를 대신하여 역할기반 접근제어가 결정한다. 개별적인 사용자는 사용자의 직무에 따라 뚜렷하게 구분되고, 각 역할에 따라 서비스 사용 승인이 다르다. 또한 사용자 역할과 역할의 권한은 다-대-다 관계로 구성된다.

역할기반 접근제어는 다양한 자격증명과 그룹별 권한 부여를 제공하지만 사용자 권한을 고려한 서비스와 데이터 접근, 정책과 사용자 프로파일 정보의 권한 식별 등을 만족시키지 못한다[5].

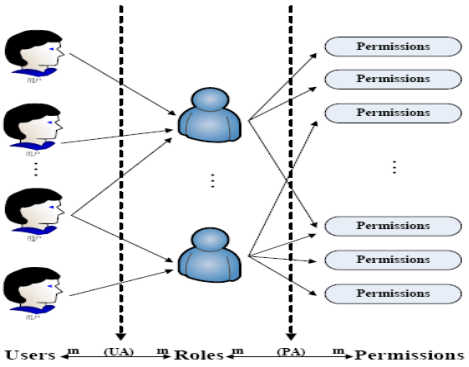

그림 4. 역할기반 접근제어 시스템

3. 클라우드 컴퓨팅 접근제어 시스템

클라우드 컴퓨팅에서의 사용자 접근제어 시스템은 기존의 클라우드 컴퓨팅 서비스 모델을 기반으로 하여 클라이언트(사용자), CoSP (Collaboration Service Provider), 3rd Party CA (Certificate Authority), CSP(Cloud Service Provider)로 구성된다. 또한 CSP는 독립적인 사용자 권한 및 보안 정책을 수립하여 관리할 수 있으며 복수의 CSP가 존재할 수 있다.

3.1 클라우드 컴퓨팅 접근제어 시스템 제안

사용자는 클라이언트를 이용하여 클라우드 서비스를 위해 CoSP에 접근요청을 한다.

CoSP는 사용자의 개인정보 보호를 위해 3rd Party CA에게 Redirection으로 사용자 인증을 수행하며 사용자가 가입된 Uer Service List Database를 기반으로 사용자가 요청한 서비스에 대한 권한을 Access Token에 부여하여 해당 클라우드 서비스 제공자의 PDP에 전달한다.

PDP에 전달된 Access Token은 CSP(Cloud Service Provider)의 PAP에서 설정한 사용자 권한 및 보안 정책에 따라 PIP는 사용자의 역할 구분 및 접근정책을 적용하여 PDP에서 Access Token의 권한 검사에 필요한 정보를 전달한다. PDP는 Security Descriptor의 Access Control List에서의 사용자 정보와 PIP의 정보를 이용하여 Access Token의 권한 검사를 수행하여 서비스 접근을 허락한다.

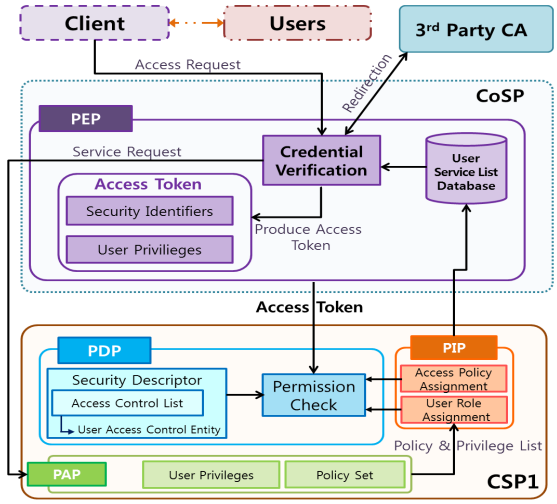

그림 5. 클라우드 접근제어 시스템

3.2 컴포넌트 정의 및 기능

• **정책 수행부 (PEP, Policy Enforcement Point)**

서비스 접근요청은 저장된 정보와 아이디, 패스워드를 통해 사용자 인증을 수행한다. 또한 정책 결정부에서 정책을 토대로 사용자의 권한 부여 승인이 이루어지면 사용자에게 접근토큰을 발행하여 서비스를 이용하도록 제공한다.

• **정책 결정부 (PDP, Policy Decision Point)**

정책 결정부(PDP)는 정책 결정에 필요한 요청 대상, 자원 또는 환경에 관한 속성값을 검색하기 위해 정책 정보부(PIP)에게 서비스를 요청할 수 있으며, 정책 결정부의 보안 기술자는 접근제어 목록, 사용자 정책 등을 고려하여 사용자의 권한 부여를 승인하고 정책 수행부에게 전달한다.

• **정책 정보부 (PIP, Policy Information Point)**

정책 정보부는 사용자의 역할 할당 및 접근 정책 할당 정보를 저장하고 있으며, 정책 결정부에게 요청 대상, 자원, 환경 등의 속성값을 검색할 수 있는 서비스를 제공한다.

• **정책 접근부 (PAP, Policy Access Point)**

정책 접근부는 정책 및 정책 목록을 작성하며 정책 결정부에서 정책이 사용가능 하도록 구성한다 또한, 관리자는 정책 접근부에서 사용자 권한을 고려한 적용 가능한 정책을 분류하여 정책 정보부에게 전송한다.

4. 결 론

본 논문에서 제안한 클라우드 접근제어 시스템은 클라우드 컴퓨팅 환경에서 사용자의 정보를 오직 인증된 기관(또는 정부기관)인 3rd party CA에게만 제공하여 사용자의 정보 노출을 최대한으로 줄였으며, 클라우드 서비스 제공자 또한 CoSP와 토큰방식의 접근요청을 통해 간편하고 독립적인 보안 정책을 보유할 수 있게 하였다.

하지만 클라우드 컴퓨팅의 기술 발전을 위해서는 본 논문에서 제안하는 클라우드 접근제어 시스템과 같은 서로 다른 서비스 제공자 및 클라우드 컴퓨팅 환경에서도 협업할 수 있는 시스템이 필요하다.

향후 연구에서는 다양한 클라우드 컴퓨팅 환경과 서비스에 따라 사용자의 정보를 최소한으로 전달하며 유연하게 서비스에 접근할 수 있는 프라이버시 접근 정책에 관한 연구를 수행할 것이다.

Acknowledgement

본 연구는 한국산업기술평가관리원(KEIT)의 연구결과로 수행되었음(10035321).

참고문헌

[1] 박준영, 나상호, 허의남, “클라우드 컴퓨팅 보안 프레임워크 연구”, 한국정보처리학회 17권 2호, 2010. 11

[2] ITU-T Focus Group on Cloud Computing. “Draft deliverable on Functional Requirements and Reference Architecture”, 2010.

[3] Verhanneman, Tine and Piessens, Frank and De Win, Bart and Truyen, Eddy and Joosen, Wouter, “Implementing a modular access control service to support application-specific policies in CaesarJ”, Proceedings of the 1st workshop on Aspect oriented middleware development, 2005.

[4] OASIS, “eXtensible Access Control Markup Language(XACML)”

[5] Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (August 1996), Role-Based Access Control Models, IEEE Computer (IEEE Press) 29 (2): 38-47.

[6] TTA, “용어사전” http://word.tta.or.kr/terms/terms.jsp