Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.573

Inter-Cloud 환경에서의 IAM 구조 및 액세스 토큰 전송 프로토콜*

김 진 욱,† 박 정 수, 윤 권 진, 정 수 환‡
숭실대학교

IAM Architecture and Access Token Transmission Protocol in Inter-Cloud Environment*

Jinouk Kim,† Jungsoo Park, Kwonjin Yoon, Souhwan Jung‡
Soongsil University

요 약

클라우드 컴퓨팅의 도입과 활용으로 클라우드 서비스를 제공하는 많은 업체가 생겨났다. 또한, 기존에 다양한 서비스 사업자들도 클라우드 형태의 서비스를 제공하기 위해 클라우드 환경으로 이동하여, 사용자들에게 클라우드를 이용한 다양한 형태의 서비스가 제공되고 있다. 이러한 클라우드 기반의 서비스를 이용하기 위하여 사용자 인증 및 인가, 관리 기술은 중요한 문제로 대두하고 있다. 특히, 타 클라우드 간 IAM(Identity and Access Management) 기술을 이용하기 위해서는 인증 및 인가 기술이 새롭게 적용되어야 한다. 이 기술은 타 클라우드 사용자 간의 손쉬운 자료 공유와 정보전달 등에 꼭 필요하다. 본 논문에서 제안하는 시스템은 사용자가 이미 가입한 기관의 인증 정보를 이용하여 타 클라우드 서비스를 이용하고자 한다. 한 기관의 클라우드 사용자가 타 기관의 클라우드 서버에 접근하여 자료를 획득하려고 할 때, 인증 정보 중 일부를 IAM 서버로 전달한다. 그 후 각 기관이 사전에 정해 놓은 Access Agreement를 이용하여 타 기관의 정보 접근 권한을 부여받는다. 사용자는 시스템을 통해 확인된 접근 권한을 토대로 타 기관의 정보에 접근할 수 있다. 이러한 방법을 이용하여 효율적이고 보안상 안전한 클라우드 간의 인증 시스템을 제안한다.

ABSTRACT

With the adoption of cloud computing, the number of companies that take advantage of cloud computing has increased. Additionally, various of existing service providers have moved their service onto the cloud and provided user with various cloud-based service. The management of user authentication and authorization in cloud-based service technology has become an important issue. This paper introduce a new technique for providing authentication and authorization with other inter-cloud IAM (Identity and Access Management). It is an essential and easy method for data sharing and communication between other cloud users. The proposed system uses the credentials of a user that has already joined an organization who would like to use other cloud services. When users of a cloud provider try to obtain access to the data of another cloud provider, part of credentials from IAM server will be forwarded to the cloud provider. Before the transaction, Access Agreement must be set for granting access to the resource of other Organization. a user can access the resource of other organization based on the control access configuration of the system. Using the above method, we could provide an effective and secure authentication system on the cloud.

Keywords: Token, Inter-Cloud, JWT, Access Agreement, IAM

Received(12. 28. 2015), Modified(05. 03. 2016), Accepted(05. 19. 2016)

* 본 연구는 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No.2015-003,클라우드 인프라 보안 강화 기술 연구)으로 수행되었음. 또한, 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터 육성 지원사업의 연구결과로 수행되었음 (IITP-2015-H8501-15-1008).

† 주저자, ouk92@ssu.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr(Corresponding author)

I. 서 론

클라우드 컴퓨팅이란 네트워크를 기반으로 소프트웨어와 하드웨어 같은 컴퓨팅 자원을 가상화하여 물리적인 서버 없이 컴퓨터 환경을 이용할 수 있는 것을 의미한다[1]. 이러한 클라우드 컴퓨팅은 물리적인 구축의 필요 없이 컴퓨팅 자원을 빌려 사용할 수 있어서 네트워크와 인프라의 초기 구축비용과 유지 보수 및 관리 비용을 절감할 수 있으며, 메모리, 디스크, 트래픽 등 컴퓨팅 자원의 갑작스러운 증가 현상에도 효과적으로 확장 및 대응할 수 있는 장점이 있다[2]. 다양한 클라우드 컴퓨팅의 장점과 네트워크 기술의 발전으로 다양한 산업 계층에서 클라우드 플랫폼의 수요가 증가함에 따라 클라우드 컴퓨팅 산업 역시 급격한 발전을 이루었다[3]. 이러한 클라우드 컴퓨팅의 발전과 이용량 증가에 따라 많은 기업과 기관의 네트워크 구조가 클라우드 환경으로 변화하였다.

보안 실무자 컨퍼런스 ISSA Forum에서 탄생한 CSA (Cloud Security Alliance)는 클라우드 컴퓨팅을 도입할 때, 고려해야 할 가이드라인을 3개 영역 14가지 항목으로 제시하였으며, 특히 클라우드 플랫폼에 심각한 위협이 될 수 있는 8가지 위협에 대해 발표하였다. 이 가이드라인에서 중요하게 다루는 위협으로는 악의를 가지고 있는 내부 관계자 (malicious insiders), 계정 및 서비스 하이재킹 (account or service hijacking) 등이 있다[4, 5]. 또한, 요즘 발생하는 APT 공격을 비롯한 많은 보안 위협의 종류가 Identity를 노리는 형태의 공격[6]과 내부 시스템에 대한 권한을 가지고 있는 정당한 인증 과정을 거친 악의적인 내부자에 의한 위협으로[7] 내부자와 클라우드 환경에서 IAM (Identity Access Management)은 더욱 중요해지고 있다.

가트너의 조사에 따르면 기업에 인기를 얻을 것으로 전망되는 클라우드 기반 보안서비스는 이메일 보안, 웹 보안, 통합계정 및 접근 관리 IAM 이며[8], 특히 IAM 시장의 경우, 연평균 약 28%의 성장률로 2013년 5억 달러, 2015년 8억6,00만 달러, 2017년 12억4,00만 달러로 확대될 것으로 전망되고 있다[9]. IAM 기술은 특히 IDaaS (IDentity as a Service) 형태로 클라우드와 함께 발전할 것으로 예상하고 있다[10,11].

최근 국내에서는 정부의 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률이 국회를 통과하였고 민간 클라우드를 공공기관에서 활용할 수 있도록 하였다. 이러한 공공기관의 클라우드 활용이 확대되면서, 안정적인 대국민 서비스를 위해 인증, 권한부여, 접근제어 기술은 필요한 기술로 대두하고 있다. 특히, 현재 상용 클라우드에서 제공하지 않는 클라우드 내에서 타 기관 클라우드(Inter-Cloud)와의 끊김 없는 자료 공유, 접근이 가능한 IAM 기술은 클라우드의 안전성, 효율성, 활용성 증대를 위해 반드시 필요한 기술이다. 특히, 타 부처 간의 협업을 위하여 기존의 다양한 인증 및 인가 기술을 결합하여 사용할 필요가 있다.

본 논문에서는 기존의 인증 및 인가 기술에서 발전한 형태의 IAM 기술을 제안하고자 한다. IAM 서비스를 이용하는 사용자는 자신이 기가입한 기관의 로그인 계정 정보를 이용하여 타 기관의 정보에 엑세스 하고자 하는 방법으로, IAM 서비스에 각 기관이 사전에 정해놓은 Access Agreement를 이용하여 자신의 계정에 대한 타 기관의 정보 접근 권한을 부여받게 된다. 이러한 방법을 이용하여 사용자는 본인이 기 속해있는 기관의 계정 정보를 이용하여, 본인이 가입되어있지 않은 타 기관에서 정보를 조회하고 자료를 다운로드 하는 등의 일을 할 수 있다.

본 논문의 2장에서는 클라우드 환경으로 변화하면서 등장한 여러 가지 클라우드 계정 관리 모델에 대하여 설명한다. 그리고 3장에서 본 논문의 Access Token으로 사용되는 Claim 기반의 JSON Web-Token에 대해 설명을 한다. 다음, 4장에서 제안하는 IAM System에 대한 구성과 용어 그리고 프로토콜을 상세하게 설명하고, 5장에서 IAM System의 특징, 기존 클라우드 계정 모델과의 비교 연구 그리고 시스템 고려사항 및 향후 연구 계획을 설명한다. 끝으로 6장에서 결론을 맺는다.

II. 클라우드 계정 관리 모델

기존 서비스와 네트워크의 환경이 클라우드 환경으로 변화하면서 바뀌면서 기존에 사용하던 계정 관리 모델 또한 클라우드 형태의 모습으로 바뀌어 연구 및 개발되고 있다[12]. 컴퓨팅 기술의 발전으로 다양한 SP (Service Provider)들이 등장하면서 사용자에게 다양한 서비스(Application)를 제공하고 있으며, 증가하는 서비스로 인한 사용자의 계정 관리 문제가 나타나기 시작했다. 이러한 사용자의 계정 관리 문제를 해결하고 더 효율적인 인증을 위하여 생겨난 IdP (Identity Provider)는 사용자가 서비스

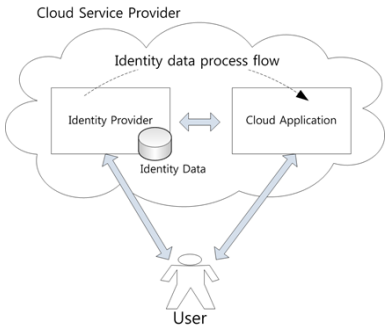

Fig. 1. Identity in the Cloud-Model

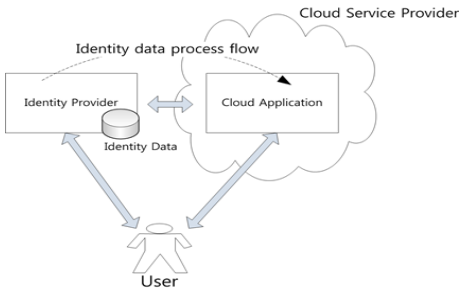

Fig. 2. Identity to the Cloud-Model

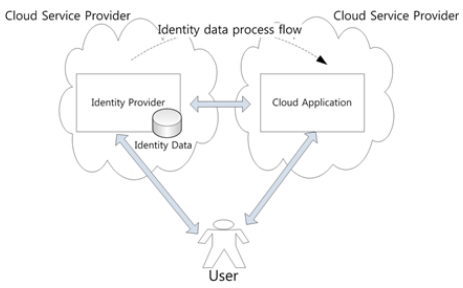

Fig. 3. Identity from the Cloud-Model

를 이용하고자 할 때, 간편한 인증 서비스가 가능하도록 지원한다. 이러한 SP와 IdP가 어떻게 배치되는지에 따라 다양한 모델들이 될 수 있다. IdP와 SP가 하나의 클라우드에 함께 구성되어있는 모델, IdP가 클라우드 서비스 형태가 아닌 클라우드 외부에 존재하는 모델, IdP와 SP가 서로 다른 클라우드 상에 존재하는 모델, IdP와 SP를 브로커가 연결해 주는 형태의 모델, 그리고 브로커 간 연결 모델이 등장 및 발전되고 있다.

본 장에서 다섯 가지 클라우드 계정 관리 모델의 형태와 특징에 관해 설명한다. 본 논문에서 제안하는 IAM System은 Cloud Identity Broker-Model과 유사한 구조를 띠며, 다음 내용에서 Broker Model에 대해 보다 자세하게 설명한다.

2.1 Identity in the Cloud-Model

Identity in the Cloud-Model은 〔Fig. 1〕과 같이 IdP와 SP가 하나의 CSP(Cloud Service Provider)에 의해 제공되고 있는 형태로 사용자의 계정 정보는 CSP 도메인에서 저장 및 관리 된다. 해당 모델을 이용하는 기관은 Identity 관리 시스템을 직접 유지와 관리 할 필요가 없어 비용 절감의 효과를 누릴 수 있지만, 사용자의 계정 정보 등의 정보를 모두 CSP에게 맡기는 것에 대한 위험부담이 따르게 된다〔12〕.

2.2 Identity to the Cloud-Model

Identity to the Cloud-Model은 Identity in the Cloud-Model과 달리, IdP가 별도로 분리된 형태로 IdP가 클라우드 외부에서 SP를 위한 Identity 관리 업무를 수행한다. IdP와 CSP의 구성은 〔Fig. 2〕와 같다. 해당 모델은 SP에게 불필요한 Identity 데이터 유출을 방지할 수 있다는 장점이 있으며, IdP가 하나의 CSP와만 연결되는 것이 아닌 다양한 CSP와 연결될 수 있어 ID 관리 인프라를 재사용할 수 있다는 장점이 있다. 하지만, 정보처리 상호 운용 관점 측면에서, IdP는 여러 CSP와 연결하기 위한 인터페이스를 구현 및 지원해야 하므로, 외부 인터페이스를 사용하는 것에 대한 개발 부담감이 증가하게 된다〔12〕.

2.3 Identity from the Cloud-Model

Identity from the Cloud-Model은 IdP와 SP가 서로 다른 클라우드 상에 독립되어 존재하는 구조의 모델로 구성은 〔Fig. 3〕과 같다. IdP는 SP와 다른 별개의 클라우드 서비스 제공 업체에 의해 운영되며, 최근 다양한 기업들에서 클라우드의 확장성과 탄력성 등의 이점을 바탕으로 IDaaS를 개발하여 서비스하고 있다. IdP를 클라우드 서비스 사업자가 운영하면서, IdP 인프라를 재사용하여 많은 SP와 연결되어 사용할 수 있다〔13〕.

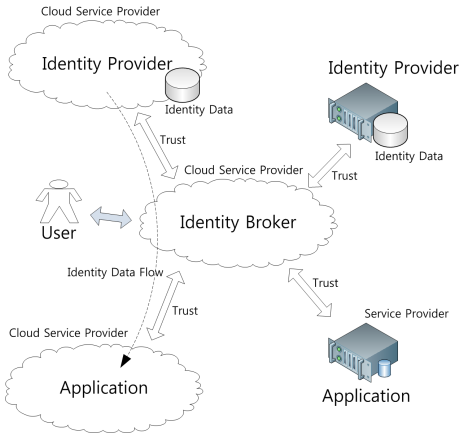

Fig. 4. Cloud Identity Broker-Model

2.4 Cloud Identity Broker-Model

클라우드 계정 브로커 모델(Cloud Identity Broker-Model)은 Identity from the cloud Model을 확장한 개념으로, 여러 SP (Service Provider)와 IdP (Identity Provider) 사이에서 브로커의 역할을 수행한다[14]. [Fig. 4] 클라우드 계정 브로커 모델에서 계정 브로커는 각각 SP, IdP와의 신뢰 관계를 전제로 하며, 여러 SP와 IdP 사이에서 이들을 연결해주는 허브 역할을 수행한다. 브로커 모델이 등장하게 된 이유는 서로 통합되고 연결된 많은 양의 IdP로부터 SP를 분리하는 것으로, SP는 사용자의 편의성과 관리의 용이성과 같은 이유로 다양한 IdP를 지원한다.

만일 SP가 계정 브로커 모델을 사용하지 않을 경우, SP는 각각의 IdP와의 통신을 위한 인터페이스를 모두 구현해야 하는 어려움이 있지만, 중앙에서 관리 및 통제를 할 수 있는 브로커 모델의 개념을 적용함으로써 SP는 계정 브로커와 연결한 하나의 인터페이스만 구현하면 되기 때문에 구현이 용이하다는 장점이 있다.

클라우드 기반의 계정 브로커는 많은 컴퓨팅 리소스와 확장성 등 클라우드의 특징 및 장점으로 인하여 많은 수의 SP, IdP와의 연결과 이들 사이에서 계정을 식별 및 인증하는 프로세스를 대신 수행할 수 있다. 그러나 클라우드 계정 브로커 모델은 사용자와 SP 모두 브로커가 지원하는 기능에 의존한다는 한계점을 지닌다.

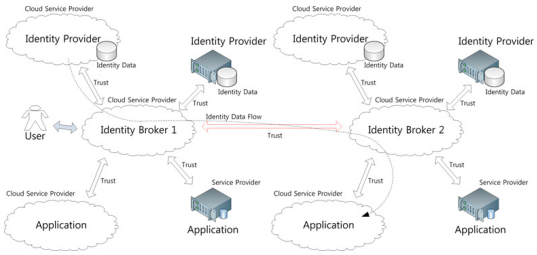

Fig. 5. Federated Cloud Identity Broker-Model

2.5 Federated Cloud Identity Broker-Model

Federated Cloud Identity Broker-Model은 Identity Broker 모델을 확장한 것으로 볼 수 있으며 구성도는 [Fig. 5]와 같다. Identity Broker 모델에서 사용자와 SP가 Broker가 제공하는 기능에 의존적이라는 한계를 해결하고자 여러 Broker를 연결한 것으로 Broker 간의 신뢰관계를 바탕으로 동작한다. [Fig. 5]에서 User는 Identity Broker 2가 지원하지 않는 IdP를 Broker 간의 연결을 통하여 이용할 수 있다[12].

III. JSON Web-Token

HTTP 프로토콜은 Stateless 속성을 지니기 때문에 브라우저와 서버는 세션과 쿠키를 사용하여 정보를 관리하고 있다. 또한, 웹 사이트가 다양한 광고와 정보들을 제공하며 복잡해지면서 CSRF (Cross-Site Request Forgery) 공격과 CORS (Cross-Origin Resource Sharing), Session 확장의 한계 등의 문제가 발생한다. 위와 같은 문제를 해결하기 위하여 제안된 JWT는 토큰 기반 인증의 한 가지 방법으로 IETF (Internet Engineering Task Force)에서 RFC 7519로 제정되었다[15].

JWT는 초창기에 통합 인증 시스템을 위한 SSO (Single Sign-On) 솔루션을 구현하는 데 사용되었다. 그리고 최근, 웹상에서 Third-Party Web Application에게 계정 정보 공유 없이 Resource Server 자원 접근이 가능하도록 Authorization을 가능하게 해주는 OAuth 2.0[16]이 JWT Bearer Token Flow를 사용할 수 있게 되면서 사용량이 증가하고 있다. 이러한 JWT는 Claim 기반의 토큰으로, Claim 정보를 JSON 형식을 이용하여 정의한다.

Claim 이란 사용자에 대한 프로퍼티나 속성이 정의되어 있는 것을 의미하고 토큰 자체가 정보를 가지고 있는 방식이다. JWT를 이용할 경우, 요청을 받은 서버나 서비스는 사용자에 대한 추가 정보를 가져올 필요 없이 토큰 안에 표시되어있는 정보만으로 원하는 정보를 충족할 수 있다. 그리고 JWT의 무결성을 보장하는 방법으로 서명(signature)이나 원본 메시지에서 해시값을 추출한 후, 이를 비밀키를 이용해 복호화시켜 토큰 뒤에 붙이는 HMAC 방식을 사용한다[17].

JWT가 무결성을 보장하기 때문에, 공격자가 메시지를 중간에서 변조했다면 변조된 메시지로 생성된 해시값과 토큰 뒤에 따라오는 HMAC 값이 달라 해당 메시지가 변조되었음을 알 수 있다. 또한, 공격자가 메시지를 변조한 후 새로운 HMAC값을 만들어 내려고 해도 HMAC은 비밀키를 이용하여 복호화되었기 때문에, 비밀키를 모르는 공격자는 HMAC을 만들 수 없다. 이러한 JWT는 헤더, 페이로드, 서명으로 구성되며 헤더 영역에는 토큰의 타입과 사용한 암호화 알고리즘이 정의된다. 그리고 페이로드에는 토큰을 이용하여 전송하고자 하는 내용이 들어있으며, 헤더와 페이로드는 base64UrlEncode되어있고 마지막 서명은 암호화 알고리즘을 사용하여 생성한 HMAC 값이다.

IV. 제안하는 IAM System

본 논문에서 제안하고자 하는 Inter-Cloud IAM System은 클라우드 서비스 사업자들 간의 Access Agreement라 하는 사전 사용자 권한 협약을 바탕으로, 사용자는 본인이 이미 보유한 한 개의 계정 정보를 이용하여 IAM System과 연결된 모든 서비스에 접근할 수 있는 것을 목표로 한다. 본 System은 서비스가 SP와 IdP의 역할을 동시에 하며, IAM Server는 이들을 중간에서 연결해주는 형태로, Cloud Identity Broker-Model과 구성은 유사하나, 역할 및 동작에 차이점이 있다. 그리고 중앙에 IAM Server가 사용자의 계정 정보를 알 수 없게 하도록, 사전에 서비스 관리자들 간 권한 협약인 Access Agreement를 이용하여 Token을 생성해서 전달한다. 본 장에서는 클라우드 서비스 사업자 간의 사용자 레벨 권한 협약인 Access Agreement에 대하여 설명을 한 뒤, 제안하는 IAM System의 구성도, 구체적인 프로토콜과 개발 후 동작 과정에 대하여 설명한다.

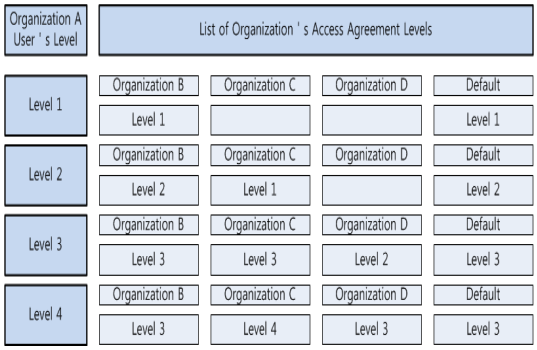

Fig. 6. Access Agreement[18]

4.1 권한 협약 (Access Agreement)

Access Agreement는 서로 다른 클라우드 서비스를 상호 연동시키기 위한 클라우드 서비스 사업자들의 사전 협약으로 설정하였다[18]. 이는 다른 서비스에 등록된 사용자들에게 자신의 서비스를 제공하기 위하여 수행하며, 각 클라우드 서비스 사용자의 레벨을 타 서비스와 대응시키는 과정이다. 이러한 과정을 이용하여 사용자는 자신이 가입되지 않은 어떠한 서비스라도 하나의 계정을 이용하여 권한에 맞는 자원에 접근할 수 있으며, 서비스 제공자는 Access Agreement를 수정함으로써 타 서비스 사용자의 권한을 쉽게 관리할 수 있다.

[Fig. 6]과 같이 Access Agreement가 맺어져 있는 경우, A 기관의 Level 1 사용자는 B 기관에서 Level 1의 권한을 얻을 수 있지만, C 기관과 D 기관은 이용할 수 없다는 것을 의미한다[18]. B, C, D 기관과 같이 세세하게 정해놓지 않은 다른 기관에는 Default 규칙이 적용되며, 위의 [Fig. 2]와 같이 맺어져 있을 때, Level 1의 권한으로 대응된다. 그리고 A 기관 Level 2의 사용자는 B 기관에서 Level 2, C 기관에서 Level 1로 대응되며, D 기관은 이용할 수 없다.

본 논문에서 예를 들어 설명한 [Fig. 6]은 A 기관의 사용자를 기준으로 나열된 것이다. 그 외 기관을 기준으로 나타내면 왼쪽 목록엔 해당 기관의 사용자 레벨이 나열되고, 다른 기관의 정보와 기본적으로 적용되는 기본 정책은 오른쪽에 나열된다.

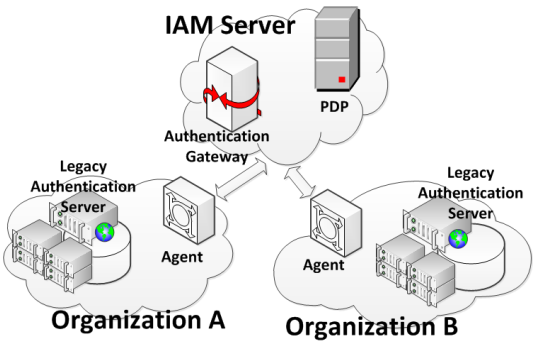

Fig. 7. Inter-Cloud IAM System Diagram[18]

4.2 IAM System 구성

본 논문에서 제안하는 Inter-Cloud System의 구성도는 [Fig. 7]과 같이 A 기관이 사용하는 클라우드와 B 기관이 사용하는 클라우드 그리고 이를 중앙에서 연결해주는 IAM Server로 구성된다[18]. 기관 A, B의 사용자 인증은 기존의 기관 서비스에서 이용해오던 인증 방식을 이용할 수 있으며, IAM Server의 AG(Authentication Gateway)는 각 기관의 로그인 사이트 정보를 가지고 사용자의 요청에 따라 이를 리다이렉트 시켜준다. 또한, PDP(Policy Decision Point)는 Access Agreement에 관한 내용이 저장되어 있으며, 사용자의 로그인 요청에 따라 Access Agreement를 바탕으로 JWT (JSON Web-Token)을 제작 및 발급의 역할을 한다. 각 기관은 처음 IAM System 등록 과정에서 서로 같은 Key를 교환한다. 기관의 관리자가 IAM System에 회원가입 및 IAM System 관리자의 승인으로 기관 관리자에게 문자열 형태의 Key가 발급되며, 이 Key는 이후 통신과정에서 발급받은 Access Token인 JWT를 검증하기 위해 사용한다. 또한, IAM System과 기관 A, 기관 B의 통신은 SSL/TLS 위에서 이루어지는 것을 전제로 한다.

4.3 인증 프로토콜

본 논문에서 제안하는 Inter-cloud 환경에서의 IAM 기술은 자신이 등록된 기관의 계정 정보를 이용하여 자신의 계정 정보가 등록되지 않은 타 기관의 자원에 엑세스 하고자 하는 방법이다.

[Fig. 8]은 A 기관의 소속된 사용자가 B 기관의

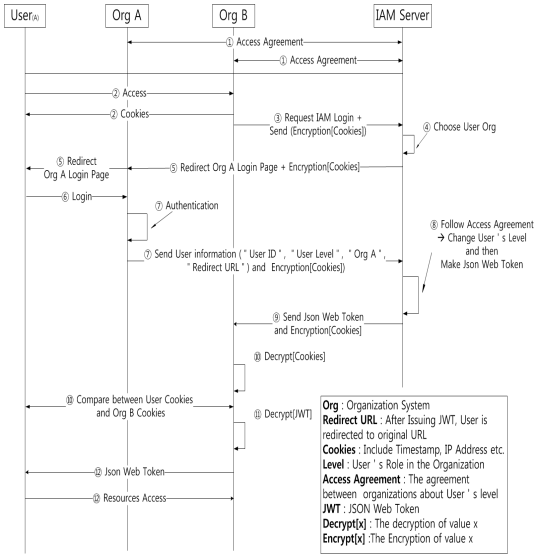

Fig. 8. Inter-Cloud IAM Authentication Flow

자료에 접근하려고 할 때의 예이다. 이를 위하여 사용자는 자신이 가입된 A 기관에서 로그인하여 최소한의 필요 정보(ID, Level, 기관정보, 로그인 시간)를 IAM 서버로 전송한다. 그리고 IAM 서버는 A 기관에서 넘어온 정보와 함께 PDP에서 이미 정의된 Access Agreement를 이용하여 JWT(JSON Web Token)을 제작하고, 이를 B 기관으로 발급하여 사용자가 정보를 획득할 수 있게 한다. 그리고 처음 사용자가 브라우저에 접속할 때, 저장되는 Cookie 값을 이용하여, 토큰 발급 후 처음에 요청했었던 사용자가 맞는지 인증하는 데 사용한다. 앞서 설명한 IAM System을 위한 구체적인 인증프로토콜을 [Fig. 8]과 함께 설명한다.

1. 기관 A에 소속되어 있는 User가 B 기관 사이트의 자료를 보기 위하여 기관 B의 사이트에 접속한다.

2. 만약, User가 자료에 액세스하기 위해 인증이 필요한 경우에 사용자는 로그인해야 하며, 로그인은 B 기관의 User가 접속하기 위한 일반 로그인과 B 기관의 계정정보를 갖고 있지 않은 IAM 서비스 사용자를 위한 로그인 방법으로 분리되어 있다.

3. 기관 B의 로그인 창에서 사용자가 IAM 서비스를 통하여 로그인을 시도할 시, 사용자의 요청 정보를 포함한 Return URL(B 기관 사이트)와 사용자의 접근 정보를 포함하는 Cookie 값을 암호화하여 IAM Server의 AG(Authentication

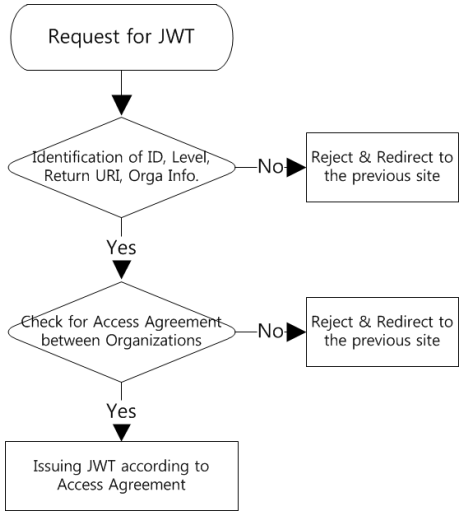

Fig. 9. JWT Issuance Flow chart

Gateway)로 리다이렉트 된다. 이때, 암호화된 Cookie 값은 추후 JWT(JSON Web Token)를 받았을 때, 초기 요청을 보낸 사용자가 맞는지 확인을 하기 위하여 사용한다.

4. IAM 사이트로 Redirect 된 User는 AG(Authentication Gateway)의 선택 리스트에서 자신이 속해있는 기관을 선택하게 된다. 예를 들기 위하여, 본 논문에서는 A 기관의 사용자가 B 기관에 접속한 것을 가정하였으므로, 사용자는 A 기관을 선택한다.

5. Authentication Gateway는 User가 선택한 A 기관의 로그인 페이지로 Redirect 시켜주게 되며, Return URL(B 기관 사이트)과 암호화된 Cookie 값을 함께 전송한다.

6. User는 자신이 속한 A 기관의 로그인 페이지에서 자신의 A 기관 회원 계정 정보를 이용하여 로그인을 수행한다.

7. 입력받은 계정 정보를 바탕으로 User가 올바른 A 기관의 사용자임이 판명되면, A 기관의 시스템에서 User의 ID, A 기관 내에서 User의 권한 Level, Return URL, 기관정보(기관 A), 암호화된 쿠키 값을 포함한 정보를 AG에 전달한다.

8. IAM Server 내에서 AG는 전달받은 정보를 PDP(Policy Decision Point)로 전달한다. PDP는 기관으로부터 넘어온 정보를 바탕으로, 〔Fig. 9〕와 같은 플로우를 따라 JWT 발급절차를 진행하게 된다. 전달받은 정보가 Id, Level, URI, Orga Info 등 필요한 정보를 포함할 경우, 두 기관 사이의 Access Agreement가 존재하는지 확인한다. 그리고 나서, PDP에서는 기존에 각 기관별로 정해놓은 Access Agreement에 의거하여 A 기관의 사용자 레벨에 따라서 해당 사용자가 B 기관에서 어떤 레벨로 권한을 사용할 수 있는지 확인한 뒤 Token을 발급하게 된다. Token은 RFC 7519에 정의된 형태로, Claim 영역에 issuer, audience, User ID, Role, token issued time, expire time, sub를 포함하게 되고 추가적으로 Cookie 값을 같이 암호화하여 전달하게 된다.

9. PDP에서 JWT를 받은 AG는 Return URL 값을 확인하여 B 기관으로 JWT를 발급하고 초기 요청을 보낸 사용자인지 확인하기 위하여 암호화된 쿠키값을 함께 보낸다.

10. JWT을 받은 B 기관에서는 건네받은 암호화된 쿠키 값과 사용자 브라우저의 쿠키값을 비교하여 초기 요청을 보낸 사용자가 맞는지 확인한다.

11. Cookie 값의 비교를 통하여 최초 접근 사용자가 맞을 경우, JWT를 디코딩하여 서명값 확인을 통해 JWT의 무결성을 확인한다.

12. JWT의 무결성을 확인한 후, 이상이 없을 경우 User에게 발급하여 권한에 맞는 자원 액세스가 가능하도록 한다.

Table 1. Configuration of Organization B

Board Name	Level
common	Level 1
information	Level 2
manege	Level 3
etc.	Admin (Level 4)

4.4 개발 내용

본 논문에서 제안하는 IAM System은 아래의 내용과 같이 구축되었다. 클라우드 서비스와 사용자를 협업을 희망하는 기관과 해당 기관에 속한 사용자로 가정하였다. 또한, 〔Table 1〕과 같이, 각 기관의 서비스는 사용자의 권한 Level 별로 이용할 수 있는 게시판과 권한이 제한되어 있으며, 구현 시스템에서도 게시판별 권한 Level을 부여하였다.

본 논문과 관련하여 구현한 IAM System의 동작 Flow Chart는 〔Fig. 10〕과 같다. 〔Fig. 11〕은 처음 기관의 사이트에 방문했을 때의 모습이다.

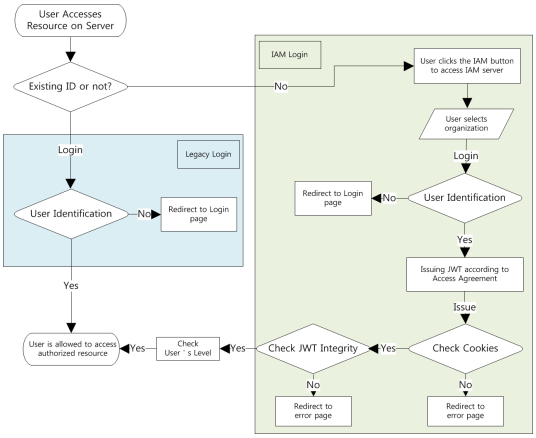

Fig. 10. IAM System Services Overview

어떠한 사용자라도 게시판을 보거나 서비스를 받기 위해서는 〔Fig. 12〕와 같이 사용자의 로그인이 요구된다. 접속한 사용자가 기관에 등록되어있는 사용자라면 본인이 계정 정보 입력을 통한 〔Fig. 10〕의 왼쪽 Legacy Login을 수행한다. 해당 기관에 계정 정보가 없는 사용자는 〔Fig. 12〕 우측에 있는 "IAM Login" 버튼을 눌러 〔Fig. 10〕 오른쪽의 IAM Login을 수행한다. "IAM Login" 버튼을 눌러 IAM Server로 리다이렉트 된 사용자는 〔Fig. 13〕과 같이 본인이 인증을 수행하고 싶은 기관을 선택하고, 〔Fig. 14〕처럼 본인이 속한 기관 시스템에 방문하여 로그인을 수행할 수 있다. 사용자의 로그인 이후, 사용자의 일부 정보가 IAM Server로 이동하여 Access Agreement 기반으로 JWT를 제작하며, 제작된 Access Token(JWT)과 함께 Return URL 값에 해당하는 처음 B 기관의 사이트로 돌아오게 된다. 사용자에게 Access Token을 주기 전에, B 기관의 시스템은 초기 접속한 사용자의 쿠키 값 비교를 통한 검증과정을 거친 후 〔Fig. 15〕와 같이 B 기관의 게시판에 접근할 수 있다.

V. 제안하는 시스템의 특징 및 평가

본 논문에서 Inter-Cloud 환경을 위한 IAM System에 대한 구성, 플로우를 제안하였다. 제안하는 IAM System은 2장에서 설명한 클라우드 계정 관리 모델 중 클라우드 계정 브로커 모델과 유사한 형태와 구성을 가진다. 중앙에서 여러 기관의 서비스들을 연결해주는 IAM Server를 두어 각 기관 서비

Fig. 11. Main Page of Organization B

Fig. 12. Organization B Requires User to Login

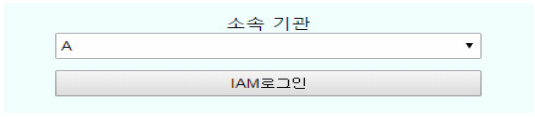

Fig. 13. User Selects Organization on IAM Server

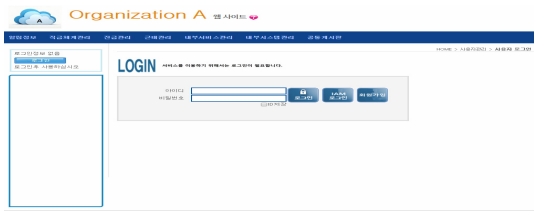

Fig. 14. User Authenticates with Organization A to Login

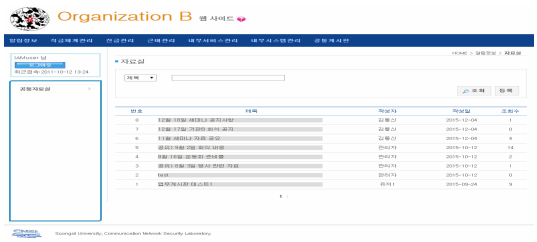

Fig. 15. After Login, User can use Organization B Services

스 간의 간접적인 신뢰 관계를 중계하며 상호 연결이 가능하게 한다. 본 장에서 제안하는 IAM System의 특징, 앞서 설명한 다섯 가지 클라우드 계정 관리 모델과의 비교 연구 그리고 IAM System의 시스템 고려사항 및 향후 연구 방향에 관해 설명한다.

5.1 특징

본 논문에서 제안하는 IAM System은 각 기관 서비스를 IAM Server가 중계하는 형태의 구성을 취한다. 새로운 서비스가 IAM service와 추가로 연결하기 위하여 기존의 연결 되어 있는 서비스를 수정하는 것이 아닌, 새로 연결을 희망하는 서비스에 IAM Server 인터페이스를 구현하는 것과 Access Agreement만으로 기존 여러 개의 서비스와 연결될 수 있다. 본 System은 Service Provider가 여러 개의 Identity Provider와 연결하기 위하여 많은 인터페이스가 있어야 하는 것이 아니라 IAM Server와 단 한 번의 연결만으로 많은 Identity Provider 및 서비스들과 연결될 수 있어 확장성이 뛰어나다. 또한, 각 서비스를 연결해주는 IAM Server는 클라우드 컴퓨팅 리소스를 이용하여 다수의 서비스가 연결되더라도 탄력적으로 서비스를 지원할 수 있다.

본 시스템은 사용자의 계정 정보가 통신상에 노출되지 않도록 JWT를 이용하여 처리하고 Access Agreement를 이용함으로써 사용자의 계정 정보를 IAM Server에 저장하지 않으며, 다른 기관에게 제공하지 않아도 된다. 또한, 기관의 서비스는 특정한 IdP에 종속되는 것이 아닌 사용자가 인증을 위하여 자신이 이용하고 있는 서비스를 이용하여 인증할 수 있는 특징이 있다. 더 나아가, 인증 플로우에 JWT를 활용함으로써 수신자가 토큰의 변조 여부를 확인할 수 있고 Expire Time을 통한 Token의 재사용을 방지할 수 있다.

IAM System을 이용하여 각 기관의 사용자는 정보 공유 및 협업을 위해 다른 기관 서비스를 이용하고자 할 때, 다른 기관 서비스에 회원가입을 하지 않아도 된다. 방문한 기관 서비스에 접근하기 위하여 본인이 속한 기관의 인증 시스템에서 인증을 받아와 허용된 범위 내의 자원 접근이 가능하다.

5.2 클라우드 계정 관리 모델과의 비교

5.2.1 비교 기준

본 논문은 다음과 같은 13가지 기준을 이용하여 여러 클라우드 계정 관리 모델과 제안하는 클라우드 IAM System을 비교한다. 클라우드 계정 관리 모델과 비교하기 위하여 선정한 비교기준은 앞선 연구들에서 이용한 비교 기준 및 정보를 인용한다[12,19,20]. 기준은 일반적인 아키텍처, 신뢰관계, 개인정보보호 등 서로 다른 영역의 측면을 대상으로 한다. 이러한 기준의 다양성은 서로 다른 클라우드 계정 관리 모델에 대한 포괄적인 개요를 제공하는 것으로 간주한다.

1. Number of SPs supported
   SP의 수를 하나로 제한하는지, 아니면 다수의 SP를 지원할 수 있는지를 확인한다.
2. Number of IdPs supported
   IdP의 수를 하나로 제한하는지, 아니면 다수의 IdP를 지원할 수 있는지를 확인한다.
3. Trust domains
   인증이 신뢰할 수 있는 도메인 내에서 제공되는지, 아니면 다른 신뢰 도메인에서 지원할 수 있는지 확인한다.
4. Trust model
   해당 모델을 직접 신뢰할 수 있는지, 아니면 누군가의 중재에 의해서 신뢰가 제공되는지 확인한다.
5. Single Sign-On
   SSO 기능을 지원할 수 있는지 확인한다.
6. Storage location of identity data
   사용자의 계정 정보가 어디에 저장되는지 확인한다.
7. Scalability
   대규모 환경에 적용될 수 있는지 확인한다.
8. Extensibility
   새로운 IdP와 SP를 추가할 때, 쉽게 확장할 수 있는지 확인한다.
9. Governance framework
   여러 요소를 포함하는 거버넌스 프레임워크인지 확인한다.
10. Cost effectiveness
    비용적인 측면에서 효과적인지 확인한다.
11. Confidentiality
    사용자의 계정 정보가 IdP와 Identity Broker에서 기밀성이 유지되는지 확인한다.

Table 2. Comparison of the individual cloud identity management-model based on selected criteria

Criterion / Model	Identity in the Cloud Model	Identity to the Cloud Model	Identity from the Cloud Model	Cloud Identity Broker Model	Federated Cloud Identity Broker Model	Proposed IAM System
Number of SPs supported	One	Multiple	Multiple	Multiple	Multiple	Multiple
Number of IdPs supported	One	One	One	Multiple	Multiple	Multiple
Trust domains	One	One	One	Multiple	Multiple	Multiple
Trust model	Direct	Direct	Direct	Brokered	Brokered	Brokered
Single Sign-On	No	Yes	Yes	Yes	Yes	Yes
Storage location of identity data	Cloud identity provider	External identity provider	Cloud identity provider	Cloud identity provider and external identity provider	Cloud identity provider and external idnetity provider	essential Identity Provider
Scalability	Medium	Low	Medium	High	High	High
Extensibility	Low	Medium	Medium	High	High	High
Governance framework	No	No	No	Yes	Yes	Yes
Cost effectiveness	Medium	Medium	Medium	High	High	High
Confidentiality	No	No	No	No	No	Yes
User Control	No	No	No	No	No	Yes
Access Control	No	No	No	No	No	Yes

12. User Control
    사용자가 자신의 계정 정보를 제어할 수 있는지 확인한다.
13. Access Control
    사용자의 권한 레벨별 액세스를 제어할 수 있는지 확인한다.

5.2.2 비교

본 논문에서 제안하는 IAM System을 앞서 제시한 13가지의 비교 기준을 이용하여 다른 클라우드 계정 관리 모델과 비교한다[12]. 다른 클라우드 계정 관리 모델과의 비교 내용은 [Table 2]에서 확인이 가능하며, 각 항목에 대한 시스템의 특징을 아래의 내용에서 설명한다.

1. Number of Sps supported
   Identity in the Cloud Model의 경우 SP와 IdP가 같은 도메인에 있으므로, IdP는 하나의 SP만을 지원한다. 그 외 다른 모델은 이러한 제약이 없으므로 계정 정보를 가지고 다양한 SP를 지원할 수 있다.
2. Number of IdPs supported
   Broker 기반의 모델 형태로 중계자 역할을 하는 요소가 있으면 다양한 IdP를 지원할 수 있으며, 그 외 다른 모델들은 하나의 IdP만 지원할 수 있다. 다양한 IdP의 지원은 사용자가 IdP를 선택하여 인증 메커니즘을 수행할 수 있게 한다.
3. Trust domains
   Broker 기반의 모델은 인증 프로세스에 참여하는 여러 요소 간 신뢰 관계를 중계하므로 여러 도메인을 신뢰할 수 있다. 또한, IAM System은 Broker 형태인 IAM Server를 통해, 본인의 시스템에서 인증을 수행하므로 신뢰도가 높다고 볼 수 있다. 그 외 모델들은 단일 도메인만을 신뢰한다.
4. Trust model
   Broker 기반의 모델은 Broker의 중계를 통해 간접적인 신뢰관계를 형성하지만, 그 외 다른 모델을 직접적인 신뢰관계를 형성한다.
5. Single Sign-On
   여러 SP를 처리할 수 있는 모델은 Single Sign-On을 적용 가능하지만, Identity in the Cloud-Model은 단순화된 Login 프로세스를 지원한다.
6. Storage location of identity data
   Identity to the Cloud-Model의 계정 정보는 외부 IdP에게 저장되며, Broker 기반 모델에서 계정 정보는 여러 다른 IdP에 분산 및 중복 저장

될 수 있다. 하지만, 중계자 역할을 하는 Broker에 직접 계정 정보가 저장되진 않는다. 그 외 다른 모델은 IdP에 직접 저장된다.
제안하는 System의 경우 계정 정보는 사용자가 속해있는 IdP에 단일 저장되며 사용자의 권한을 대응할 수 있도록 해주는 Access Agreement에 관한 내용은 IAM Server(Broker)에 저장된다.

7. Scalability
Identity to the Cloud-Model은 다른 외부 IdP를 이용할 수 없도록 설계되어 유동성 및 탄력성이 부족하여 대규모 환경에 적용하기 어렵다. 그 외, 다른 모델들은 대규모 환경에 적용할 수 있으며 Broker 모델 및 본 논문에서 제안하는 IAM System은 높은 수준의 대규모 환경에 적합함을 가지고 있다.
8. Extensibility
Identity in the Cloud-Model은 SP와 IdP가 하나의 도메인에 있기 때문에 확장할 수 없으며, Identity to the Cloud-Model, Identity from the Cloud-Model은 추가적인 SP의 통합을 통한 확장이 가능하다. 그리고 Broker 기반의 두 모델과 IAM System은 많은 SP와 IdP를 확장 가능하여 높은 수준의 확장 가능 능력을 가지고 있다.
9. Governance framework
직접적으로 연결되는 신뢰 모델은 광범위한 거버넌스 프레임워크를 필요로 하지 않는다. Broker 기반의 거버넌스 프레임워크는 다양한 공급자의 상호작용을 가능하게 한다.
10. Cost effectiveness
Broker 형태의 모델은 Cloud 형태로 여러 IdP와 연결 및 재사용이 가능하므로 가장 높은 비용 효과가 있다. 외부 IdP를 재사용 하는 것은 비용을 아낄 수 있지만, 단지 IdP가 클라우드 형태로 배포되는 모델은 큰 혜택을 누릴 수 없다. Broker 형태 외의 다른 모델들은 중간 정도의 비용 효과가 있다.
11. Confidentiality
제안하는 IAM System은 SSL/TLS를 이용한 통신을 전제로 하여 통신상의 기밀성을 확보할 수 있으며, 처음 요청한 사용자가 맞는지 확인을 통하여 안전한 통신이 가능하도록 한다. 또한, JSON Web-Token을 이용한 무결성 체크가 가능하다. 그 외, 다른 모델들은 평문 형태로 값을 전달하여 기밀성을 유지하는 데 한계가 있을 수 있다.
12. User Control
본 논문에서는 모든 User Control이 신뢰할 수 있는 IdP에서 가능함을 전제로 한다. IAM System의 경우, 본인이 기 가입하여 사용한 기관의 시스템 인증 방식을 이용함으로 신뢰할 수 있다. 또한, 직접 기관에 접속하여 정보를 수정할 수 있다.
13. Access Control
IAM System은 Access Agreement라 불리는 서비스 관리자간 사전 권한 협약을 통하여 다른 시스템 및 기관의 사용자가 접근 할 수 있도록 지원하며, 이후 Access Agreement 변경 및 삭제를 통하여 다른 시스템 사용자에 대한 접근을 제어할 수 있다. 그 외, 다른 인증 모델은 사용자를 인증하기 위한 IdP와 SP의 구성에 대한 것으로 IdP에서 지원하는 범위의 Access Control을 따른다.

5.3 시스템 고려사항 및 향후 연구계획

본 논문에서 제안하는 IAM System은 SSL/TLS의 사용을 전제로 한다. 각 기관의 서비스 및 IAM Server는 SSL/TLS를 이용하여 통신상의 기밀성을 확보할 수 있으며 안전한 통신이 가능하게 한다. 또한, IAM System은 초기 각 기관의 관리자가 IAM System의 연결 및 Access Agreement 단계에서 서비스에 고유한 Key를 발급받으며, 이 Key를 이용하여 암호화한 Cookie 값의 비교를 통해 초기 요청을 보낸 사용자가 맞는지 검증하는 과정이 있다. 그리고 앞서 발급받은 Key를 이용하여 IAM Server로부터 발급받은 JWT의 무결성을 검증하는 데 이용할 수 있다.

하지만, 본 논문에서 제안하는 IAM System은 IAM Server와 연결하고자 하는 각 기관의 클라우드 서비스가 인터페이스 연결 및 토큰을 이용한 자원에 액세스를 하기 위해 기관 서비스의 수정 및 추가적인 구현이 불가피하다는 점이 있으며, 최종 사용자에게 전달된 JWT의 Expire Time이 지나기 전에 재사용 공격에 이용될 수 이 있는 한계가 존재한다.

향후 연구에서 Expire Time 내에 다른 사용자의해 행해지는 재사용 공격을 방어하는 기법을 연구

하며, 전체적인 시스템의 성능 및 고도화를 위한 연구가 진행될 예정이다.

VI. 결 론

본 논문에서는 타 클라우드 서비스, 타 기관과의 정보전달을 안전하고 효율적으로 할 수 있는 Inter-cloud 내의 IAM 아키텍처에 대하여 제안하였다. 기존의 타 기관의 자료를 공동 활용할 경우 타 기관의 사이트에 회원가입을 하고, 인증해야 하는 불편함이 있었으며, 제공되는 정보에 대한 제한을 일일이 두어야 한다는 점에서 불편함이 있었다.

하지만, 본 논문에서 제안하는 아키텍처를 통하여 기존의 사용자가 타 사이트에 가입할 필요 없이 IAM 서버를 통하여 기존 계정 정보를 활용하여 본인을 인증하고, 타 서비스의 자원과 정보를 이용할 수 있다는 점에서 더욱 효율적으로 사용 가능한 시스템을 설계하였다. 이러한 시스템을 이용하여 사용자는 서비스를 이용하기 위하여 회원가입을 하는 것이 아닌, 기존 본인의 등록된 기관 및 서비스에서 인증을 수행함으로써 새로운 서비스 이용이 가능하다. 그리고 서비스 관리자는 시스템과 서비스를 연결할 때, 권한 협약 및 인터페이스 연결로 다른 많은 서비스와 쉽게 연결할 수 있다. 또한, 서비스 관리자는 권한 협약을 수정함으로써 타 서비스 사용자에 대한 손쉬운 관리가 가능하다.

정부에서 민간 클라우드를 공공에 사용하려고 할 때, 정보와 자원을 얼마나 제공할지에 대한 공개 범위, 민간 클라우드를 통해서 들어온 사용자에 대한 인증 및 인가 방법 등은 매우 중요한 문제가 될 수밖에 없다. 따라서 제안하는 시스템을 통하여 민간 클라우드 혹은 타 기관 간의 인증 및 인가 프로세스가 이루어질 경우, 더욱 안전하고 효율적으로 사용 가능할 것으로 생각된다.

References

[1] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing," IEEE International Conference on Cloud Computing, pp. 109-116, Sep. 2009.

[2] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of network and Computer Application, vol. 10, no.2, pp. 1-11, Jan. 2011.

[3] J. Lee, J. Son, H. Kim and H. Oh, "An Authentication Scheme for Providing to User service Transparency in Multi cloud Environment," Journal of the Korea Institute of Information Security and Cryptology, vol. 23, no. 6, pp. 1131-1141, Dec 2013.

[4] Cloud Security Alliance, "Security Guidance for critical areas of focus in cloud computing v3.0", https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, Nov 2011.

[5] Cloud Security Alliance, "Top Threats to Cloud Computing Survey Results Update 2012", https://downloads.cloudsecurityalliance.org/initiatives/top_threats/Top_Threats_Cloud_Computing_Survey_2012.pdf, 2012.

[6] K. Son, T. Lee and D. Won, "Design for Zombie PCs and APT Attack Detection based on traffic analysis," Journal of the Korea Institute of Information Security and Cryptology, vol. 24, no. 3, pp 491-498, Jun 2014.

[7] A. Mahajan, S. Sharma, "The Malicious Insiders Threat in the Cloud," International Journal of Engineering Research and General Science, vol. 3, no. 2, pp. 245-256, Mar-Apr. 2015.

[8] D. M. MANGIUC, "Cloud Identity and Access Management - A Model Proposal," In Proceedings of the 7th International Conference Accounting and management information systems AMIS, pp. 1014-1027, Jun. 2012.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol.

IT-22, no. 6, pp. 644-654, Nov 1976.
〔10〕 A. Gopalakrishnan, "Cloud computing identity management," SETLabs briefings 7.7, pp. 45-55, 2009.
〔11〕 Varia, Jinesh. "Best practices in architecting cloud applications in the AWS cloud," Cloud Computing: Principles and Paradigms, pp 459-490, 2011.
〔12〕 B. Zwattendorfer, T. Zefferer and K. Stranacher, "An Overview of Cloud Identity Management-Models," WEBIST 2014, pp. 82-92, Apr. 2014.
〔13〕 M. Ates, S. Ravet, A. M. Ahmat, and J. Fayolle, "An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and other delights," ARES 2011, pp. 555-560, Aug. 2011.
〔14〕 B. Zwattendorfer, K. Stranacher, and A. Tauber, "Towards a Federated Identity as a Service Model," Lecture Notes in Computer Science, pp. 43-57, 2013.
〔15〕 M. Jones, J. Bradley, N. Sakimura, "JSON Web Token (JWT)," Internet Engineering Task Force (IETF) RFC 7519, May. 2015.
〔16〕 D. Hardt, Ed.,"The OAuth 2.0 Authorization framework," Internet Engineering Task Force (IETF) RFC 6749, Oct. 2012.
〔17〕 H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," Internet Engineering Task Force (IETF), Feb. 1997.
〔18〕 J. Kim, J. Park, M. Park and S. Jung, "IAM Clustering Architecture for Inter-Cloud Environment," The Journal of Korean Institute of Communications and Information Sciences, vol. 40, no. 5, pp. 860-862, May. 2015.
〔19〕 D. Nunez, I. Agudo and J. Lopez, "Leveraging Privacy in Identity Management as a Service through Proxy Re-Encryption," ESOCC 2013, pp. 42-47, Sep. 2013.
〔20〕 E. Birrell and F. B. Schneider, "Federated Identity Management System: A Privacy-Based Characterization," IEEE Security and Privacy, vol. 11, no. 5, pp. 36-48, Sep. 2013.

〈저자소개〉

김 진 욱 (Jinouk Kim) 학생회원
2014년 2월: 숭실대학교 평생교육원 컴퓨터공학과 졸업
2014년 9월~현재: 숭실대학교 정보통신공학과 석사과정
〈관심분야〉 클라우드 보안, IoT 보안, 사용자 및 디바이스 인증

박 정 수 (Jungsoo Park) 학생회원
2013년 2월: 숭실대학교 정보통신전자공학부 졸업
2015년 2월: 숭실대학교 전자공학과 석사
2015년 3월~현재: 숭실대학교 융합SW공학과 박사과정
〈관심분야〉 클라우드 보안, 모바일 보안, 네트워크 보안, 사용자 및 디바이스 인증

윤 권 진 (Kownjin Yoon) 학생회원
2015년 2월: 숭실대학교 정보통신전자공학부 졸업
2015년 3월~현재: 숭실대학교 정보통신공학과 석사과정
〈관심분야〉 클라우드 보안, 네트워크 보안, 사용자 및 디바이스 인증

정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 졸업
1987년 2월: 서울대학교 전자공학과 석사
1996년 6월: University of Washington 박사
1988년~1991년: 한국통신 전임 연구원
1997년~현재: 숭실대학교 전자정보공학부 교수
〈관심분야〉 클라우드 보안, 모바일 보안, 네트워크 보안