클라우드 컴퓨팅 환경에 적합한 사용자 중심의 ID관리기술

황문영*, 곽진*

요약

클라우드 컴퓨팅은 가상화를 통해 인터넷에 있는 일부 또는 모든 IT자원을 아웃소싱하는 형태로써 현재 가장 주목 받는 기술 중의 하나이다. 이와 같은 클라우드 컴퓨팅 환경에서는 서비스 이용 시 사용자 식별 ID를 효율적으로 관리하기 위해 ID Federation 기술이 사용되고 있다. 하지만 ID Federation 기술은 사용자의 개인정보에 대한 사용자 중심의 관리 수단을 제공하고 있지 않기 때문에, 악의적인 공격자에 의한 개인정보의 도용 및 프라이버시 침해 등이 일어날 수 있다. 따라서 본 논문에서는 클라우드 컴퓨팅 환경에서 보안성과 자기정보통제권을 동시에 제공하는 사용자 중심의 ID관리기술에 대해 제안한다.

User-Centric ID Management Technique for Cloud Computing

Moon-Young Hwang*, Jin Kwak*

ABSTRACT

The Cloud Computing is one of the attention techniques which outsourcing of IT resources. It used ID Federation for efficient management of user's recognition ID on services. However, ID Federation is not offering management system of user privacy information for managed himself/herself. Thus, user suffer a great damage such as invasion of privacy or plagiarize user information from a malicious attacker. In this paper, we propose user-centric ID management technique that provide security and right to control own information in cloud computing environment.

Key Words : Cloud computing, ID Management, SSO, OpenID, User-Centric

* 순천향대학교 정보보호학과
· 제1저자(First Author) : 황문영 · 교신저자(Correspondent Author) : 곽 진
· 접수일(2010년 1월 11일), 수정일(1차 : 2010년 2월 10일), 게재확정일(2010년 2월 12일)

www.kci.go.kr

Ⅰ. 서 론

현재 IT 기술은 시간과 공간의 제약성을 극복하기 위해 새로운 컴퓨팅 환경에 대한 연구가 활발히 진행되고 있다. 이와 같은 연구를 통해 인터넷을 활용하여 가상화된 IT 자원을 서비스로 제공하고, 특정 자원들을 필요한 만큼 사용 한 후 비용을 지불하는 클라우드 컴퓨팅 개념이 등장하게 되었다. 클라우드 컴퓨팅 환경에서 제공되는 다양한 서비스를 이용하기 위해서는 기존의 인터넷 서비스와 동일하게 사용자의 개인정보를 제공하고 ID를 발급받아야 한다. 이는 사용자들이 사용하는 클라우드 서비스가 증가함에 따라 사용자가 관리해야 하는 ID정보도 증가한다는 것을 의미한다. 따라서 사용자의 ID를 효율적으로 관리하고, IT자원의 가상화를 통해 개별적으로 구성되는 시스템간의 SSO(Single Sign-On) 기능 등을 제공하는 ID관리 기술의 필요성이 증가하게 되었다.

이를 위해 현재 대부분의 클라우드 시스템에서는 ID Federation방식의 기술[1]을 사용하고 있다. 이 ID Federation방식은 사용자가 데이터에 안전하게 접근할 수 있고, 서로 다른 클라우드 시스템간의 상호 정보 교환을 통해 사용자가 한 번의 로그인으로 서비스간의 이동이 있을 때 재인증이 필요 없는 SSO 기능을 제공하며, ID를 생성하고 ID정보를 관리하는 기능을 제공한다. 하지만 ID Federation방식은 사전 협약에 의해 연합한 사업자들의 서비스에서만 상호 정보 교환이 이루어지고 개인정보의 통제에 대한 모든 권리가 서비스 제공자에게 이양되어 개인정보에 대한 사용자의 통제권이 없다는 문제점이 있다. 이와 같은 이유로 사용자가 개인정보에 대한 자기정보통제권을 가지고 개인정보의 도용과 프라이버시 침해를 막을 수 있는 새로운 ID관리 기술이 필요하다.

본 논문에서는 사용자가 클라우드 컴퓨팅 환경에서 다양한 정보 시스템에 접근할 때에 사용자에게 한 번의 인증과정을 거침으로써 이기종의 정보 시스템간의 이동이 가능하게 하고 보안성을 제공하며 사용자에게 자기정보통제권을 제공하는 ID관리기술을 제안하고자 한다. 이를 위해 2장에서는 클라우드 컴퓨팅과 현재 사용되고 있는 ID관리기술들에 대해 설명을 하고, 3장에서는 관련연구에 대한 문제점을 분석하였다. 4장에서는 클라우드 컴퓨팅 환경에 적합한 사용자 중심의 ID관리 모델을 제안하고, 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1 클라우드 컴퓨팅 개요

클라우드 컴퓨팅 환경에서 서비스 제공자는 여러 곳에 분산되어 있는 물리적 인프라를 가상화하여 가상의 자원풀(Resourece Pool)을 구축하고 사용자의 작업요구수준(Workload)에 따라 이러한 자원들을 효율적으로 배분한다. 또한 사용자들은 서비스 제공자가 제공하는 카탈로그를 통해 서비스를 요청하고, 서비스 제공자의 시스템 관리 모듈은 이 같은 요청에 대해 가상화된 서버 네트워크를 통해 필요한 리소스를 조달하게 된다. 사용자는 클라우드 컴퓨팅 시스템에 인증을 하고 자신이 필요한 서비스를 이용할 뿐 어떻게 서비스가 제공되고, 자신의 데이터와 정보가 어디에 보관되는지, 어느 곳에 위치한 서버가 활용되는지 등의 세부적인 정보는 알지 못한다. [2][3]

그림 1. 클라우드 컴퓨팅의 구조
Fig 1. Architecture of Cloud Computing

www.kci.go.kr

클라우드 컴퓨팅의 서비스는 사용자가 요청하는 자원의 종류에 따라 다양하게 분류 될 수 있지만, 대표적인 서비스로서 IaaS, Saas, PaaS가 있다.[4][5]

표 1. 클라우드 컴퓨팅의 서비스 유형
Table 1. Type of Cloud Computing Service

서비스 유형	설 명
IaaS(Interface As A Service)	서버 또는 스토리지를 사용자에게 서비스 형태로 제공하는 클라우드 컴퓨팅 서비스
Paas(Platform As A Service)	사용자가 쉽게 서비스를 만들 수 있도록 필요한 기본 기능을 제공하는 플랫폼을 서비스 형태로 제공
SaaS(Software As A Service)	어플리케이션을 서비스 형태로 제공하는 서비스

2.2 가상화 기술 개요

클라우드 컴퓨팅 환경에서 가상화란 물리적으로 시스템을 논리적으로 통합하거나 하나의 시스템을 논리적으로 분할해 자원을 효율적으로 사용하게 하는 기술로 정의할 수 있다. 즉, 가상화는 컴퓨터 자원을 추상화한다는 의미이며 자원을 다루는 어플리케이션이나 사용자에게 복잡한 물리적인 속성을 숨기고 논리적인 자원을 보여주는 기술을 의미한다.

IT자원의 가상화는 시스템 운용의 효율성을 제공하고, 새로운 App, 보안정책, 운영체제의 적용을 쉽고 빠르게 할 수 있다.

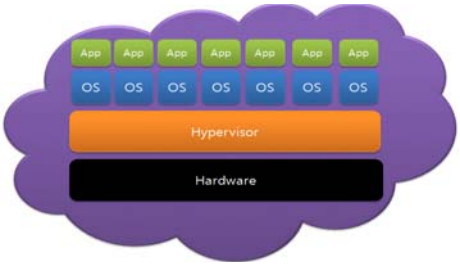

그림 2. 가상 시스템 환경
Fig 2. Environment of Virtual System

2.3 ID관리기술

2.3.1 SSO(Single Sign-On)

SSO는 모든 인증을 하나의 시스템에서 하는 접속 기술이다. 즉 접속하고자 하는 정보 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공을 하면 다른 시스템에 대한 접근 권한도 부여 받아 재인증 절차 없이 서비스를 받을 수 있다. [6][7]

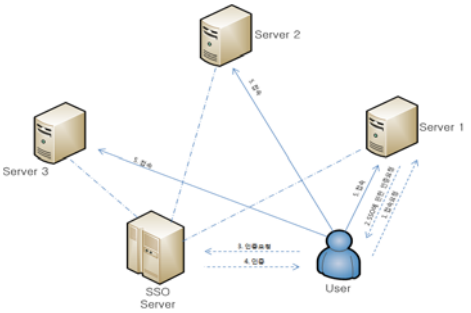

그림 3. SSO 인증 절차
Fig 3. Authentication Procedure of SSO

(1) 사용자가 서버에 연결 요청
(2) 서버는 사용자가 SSO 서버로부터 인증을 받은 후 접속하도록 요청
(3),(4) 사용자가 SSO 서버에게 인증 받음
(5) SSO 서버와 연결된 서버 1,2,3에 별도의 인증 과정 없이 접속 가능

2.3.2 OpenID

OpenID는 하나의 ID로 OpenID 인증 프로세스가 적용된 모든 서비스에 별도의 가입 없이 로그인 되는 프로세스를 말한다. 즉, 하나의 로그인 계정으로 모든 서비스를 이용할 수 있게 한다는 Single Sign-On의 개념을 구체화한 기술이다. 인터넷 사용자들은 자신의 ID정보를 관리하기 위해 하나의 서비스 제공자에게 의존할 필요가 없으며, 어느 기업의 서비스든 웹 주소

www.kci.go.kr

를 ID로 이용해 로그인을 할 수 있다. 게다가 자신의 이름과 주소 등의 개인정보를 계속 입력할 필요가 없으며, 사용자가 가지고 있는 ID정보를 분실할 위험이 없다. 이로써 사용자는 단 하나의 계정만 관리하면 되고 그에 따라 패스워드의 길이와 복잡도는 높아질 수 있게 된다.

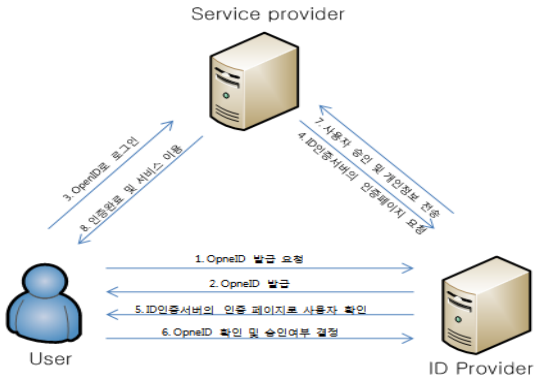

그림 4. OpenID 동작 절차
Fig 4. Operation Procedure of OpenID

사용자 중심의 새로운 ID관리기술인 OpenID는 IDP(ID Provider)를 이용해 인증을 제공하는데 ID이외에 추가적인 정보를 필요로 하지 않고 OpenID인 URL만 가지고 사용자를 인증한다.

OpenID는 일반적인 ID관리기술과 비교해서 몇 가지의 특징들을 가지게 되는데 첫째로 중앙 집중화된 구조가 아니라 분산되어 있다는 것이다. 이는 누구나 IDP가 될 수 있으며, 이를 위해 중앙의 어떤 것으로부터의 허가나 등록이 필요 없다는 것을 의미한다. 또한 사용자는 자신이 사용하고자하는 IDP를 선택할 수 있고, IDP를 변경할 경우에도 ID를 유지할 수 있다.

둘째로 OpenID를 사용할 수 있는 모든 웹 사이트에서 사용이 가능함으로써 첫 로그인으로 이용할 수 있는 서비스의 영역이 확장된다. 셋째로 OpenID는 부가적인 ID의 요청 없이 온라인상에서 기존의 웹 브라우져를 이용해 개인에 대한 인증을 수행한다. [8][9][10]

III. 문제점 분석

3.1 OpenID기술의 신뢰성 부재

OpenID는 가입자 정보를 중앙에 집중시켜 관리하는 형식이 아닌 분산 구조로 이루어져 있다. 따라서 누구나 IDP가 될 수 있으며, 이를 위해 중앙으로부터 허가나 등록 과정이 필요 없다는 것을 의미한다. 그러나 이러한 특징으로 인해 IDP의 신뢰성이 다른 ID관리 기술에 비해 낮고, 이를 통해 발급된 ID의 진정성 및 보안성 또한 취약하다. 결국 악의적인 목적을 지닌 공격자가 IDP를 구축하고 그 곳에서 발급된 ID를 이용하여 정당한 사용자로 위장해 서비스에 접근할 수 있다는 문제점이 존재한다. 이런 문제점은 작게는 스패밍(Spamming), 크게는 서비스거부공격으로까지 이어질 수 있다.

3.2 자기정보통제권의 부재

다수의 서비스 제공자들은 사용자들이 서비스를 제공받고자 할 때 서비스 이용에 필요한 것 이상의 개인정보를 요구한다. 하지만 서비스를 제공받기 위해서는 모든 정보를 입력해야 한다. 또한 자신의 개인정보를 각 정보 시스템마다 개별적으로 입력을 해야 하며 자신의 개인정보임에도 불구하고 클라우드 컴퓨팅 환경의 가상화 특성으로 인해 자신이 통제할 수 없는 상황이다. 이로 인해 자신의 개인정보가 어디에 저장되었는지 알지 못하고, 사용자 자신도 모르는 사이에 개인정보의 도용이나 프라이버시 침해로 이어질 수 있다.

IV. 사용자 중심의 ID관리 기술

본 장에서는 클라우드 컴퓨팅 환경에서 적절한 보안성과 자기정보통제권 그리고 SSO기능을 제공하는

www.kci.go.kr

사용자 중심의 ID관리 기술을 제안한다. 제안된 ID관리 기술의 기본 동작은 다음과 같다.

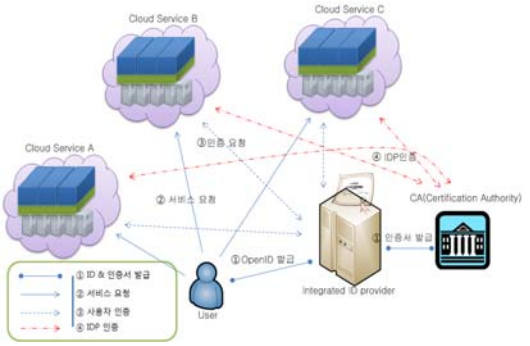

그림 5. 제안 기술의 동작 과정
Fig 5. Operation Procedure of Proposal Method

제안한 ID관리 기술을 클라우드 컴퓨팅 환경에 적용하기 위하여 자신의 개인정보를 저장하고 OpenID를 발급/인증해주는 IIDP(Integrated ID Provider), IIDP에게 인증서를 발급해주는 신뢰기관 CA(Certification Authority)가 필요하다. 이 때 CA는 충분히 신뢰할만한 기관이라고 가정한다.

4.1 제안된 ID관리 기술의 프로토콜

4.1.1 사용자 ID발급 절차

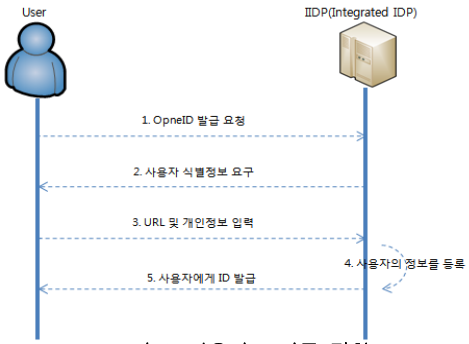

그림 6. 사용자 ID발급 절차
Fig 6. Issuance Procedure of User ID

(1) 사용자는 IIDP에게 ID(URL) 발급 요청을 한다.
(2) IIDP는 사용자에게 ID로 사용할 사용자 식별정보를 요구한다.
(3) 사용자는 IIDP에게 ID로 사용할 실제로 존재하는 자신의 URL 및 패스워드를 포함한 개인정보를 SP에게 전송한다.
(4) IIDP는 사용자의 정보를 저장한다.

위 프로토콜은 사용자와 IIDP간의 회원 가입 절차이다. 이때 사용자가 IIDP에게 URL과 함께 제공하는 개인정보는 다양한 서비스를 사용할 때에 필요한 정보들을 의미한다. 예를 들면 결혼정보업체의 경우 나이, 사진, 학벌 및 수입 등의 다양한 정보가 필요할 것이고 쇼핑몰 같은 경우는 자신의 주소와, 연락처 등의 간단한 정보만 필요로 할 것이다.

다음은 발급 받은 ID를 가지고 서비스를 제공받는 프로토콜을 나타낸 것이다.

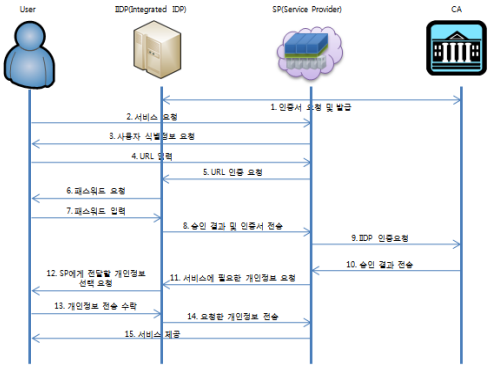

그림 7. 서비스의 절차
Fig 7. Procedure of Service

(1) IIDP는 신뢰기관 CA에게 자신의 정당함을 검증해 줄 인증서를 요청 및 발급 받는다.
(2) 사용자는 SP에게 서비스를 요청한다.
(3) SP는 사용자에게 인증에 사용할 사용자 식별 정보를 요청한다.

www.kci.go.kr

표 2. 클라우드 컴퓨팅 환경에서 ID관리 기술의 비교
Fig 2. Comparison of ID Management in Cloud Computing Environment

비교항목	ID Federation	OpenID	제안된 ID관리 기술
확장성	X	O	O
자기정보통제권	X	X	O
IDP 인증	O	X	O
SSO	O	O	O

(4) 사용자는 SP에게 IIDP에게 등록한 URL을 입력한다.
(5) SP는 사용자에게 전송받은 URL을 IIDP에게 인증 요청을 한다.
(6) IIDP는 전송 받은 URL의 정당한 사용자임을 인증하기 위해 사용자에게 PW를 요청한다.
(7) 사용자는 IIDP에게 패드워드를 전달한다.
(8) IIDP는 패스워드를 비교하여 승인결과와 자신의 인증서를 SP에게 전송한다.
(9) SP는 사용자를 인증한 IIDP가 정당한 IIDP인지 신뢰하는 CA에게 IIDP 인증 요청을 한다.
(10) CA는 인증서를 바탕으로 IIDP에 대한 인증 결과를 SP에게 전달한다.
(11),(12) SP는 사용자에게 서비스를 제공하기 위해 필요한 개인정보를 IDP에 요청을 하고, IIDP는 사용자에게 SP에게 전달할 개인정보의 종류를 선택하게 한다.
(13) 사용자는 저장된 목록 중에 SP에게 전송할 개인정보를 선택 후 수락을 한다.
(14),(15) IIDP는 사용자가 선택한 개인정보를 SP에게 전송하고 SP는 사용자에게 서비스를 제공한다.

위의 (1)의 과정은 IIDP가 자신이 정당한 IDP라는 것을 SP에게 증명하기 위해 신뢰기관 CA에게 인증서를 발급받는 과정이다. 이 과정은 IIDP가 인증서를 가지고 있지 않을 때 한번만 유효하며 인증서의 유효기간이 만료되기 전까지 과정을 진행할 필요가 없다. (2)~(15)까지의 과정은 사용자가 SP에 서비스 요청을 했을 때 이뤄지는 절차이다. 만약 저장된 개인정보의 수정이 필요할 경우 사용자는 IIDP에 저장된 개인정보를 수정한 후 SP에게 자신의 개인정보가 변경되었음을 (15)번 과정 이 후에 알리고 (11)~(14)과정의 수행을 요청한다. IIDP의 인증서를 바탕으로 이루어지는 CA와의 통신은 매 접속마다 이루어져야 하는데 그 이유는 CA가 발급한 인증서의 유효기간의 확인과 사용자가 IIDP를 변경했을 경우를 위함이다.

위에서 제안된 사용자 중심의 ID관리 기술은 클라우드 컴퓨팅 환경에서 필요로 하는 요구사항을 모두 만족한다. 사용자는 IIDP를 통해 SP에게 제공해줄 개인정보를 직접 관리하고 제어를 할 수 있으며, 신뢰기관 CA로부터 인증서를 받은 IIDP를 통해 SP에게 정당한 IIDP임을 보여줄 수 있다. 이는 현재 사용되고 있는 ID연계 방식의 기술이 가지고 있는 문제점을 해결했다고 볼 수 있다.

Ⅴ. 기존의 ID관리 기술과 비교

- 확장성 : 확장성이란 서로 다른 프로토콜을 가지고 있는 클라우드 시스템간 상호 정보 교환 능력을 말한다. 기존 ID Federation 방식은 서로 같은 프로토콜 상에서만 데이터 송수신이 가능하다. 그러나 OpenID나 제안된 ID관리 기술은 서로 다른 프로토콜을 지닌 클라우드 시스템 사이에서 데이터 송수신이 가능하다.

- 자기정보통제권 : 자기정보통제권이란 사용자 스스로 자신의 개인정보를 관리할 수 있는 권리를 말한

www.kci.go.kr

다. ID Federation의 경우 사용자 중심이 아닌 연계된 클라우드 시스템 중심의 ID관리 기술이므로 사용자의 모든 개인정보를 IDP가 관리하기 때문에 자기정보통제권을 제공하지 못한다. 또한 OpenID 기술은 IDP에게 발급받은 URL을 사용하여 서비스에 간단한 인증 작업만 수행할 뿐 개인정보를 다루지는 않는다. 반면, 제안된 ID관리 기술은 IIDP에 사용자의 개인정보를 저장하여 서비스를 제공받기 위한 최소한의 정보 제공을 수행하며, 저장된 개인정보에 대한 등록, 수정, 삭제 등의 관리가 용이하다.

- IDP 인증 : OpenID에서 IDP는 URL에 대한 단순 인증기능만 제공할 뿐, IDP의 정당성 여부는 확인할 수 없다. 하지만 ID Federation의 경우 SP가 IDP의 역할을 수행하므로 신뢰성을 보장이 되며, 제안된 ID관리 기술은 신뢰기관 CA를 통해 자신을 인증하게 되므로 정당한 IDP임을 인증할 수 있다.

- SSO : 사용자가 한 번의 로그인으로 편리하게 서비스를 제공받을 수 있게 하는 SSO 기술은 ID Federation, OpenID, 제안된 ID관리 기술 모두 제공한다.

Ⅵ. 결론

클라우드 컴퓨팅 환경의 등장은 네트워크 환경을 통해 서비스를 이용하는 모든 사용자에게 이슈가 되었다. 클라우드 컴퓨팅은 가상화된 공간에 어플리케이션, 스토리지, 인프라의 일부 또는 모든 IT자원이 아웃소싱 형태로 구성이 되어 사용자가 단말의 컴퓨팅 파워나 어플리에션의 설치 유무에 상관없이 어디에서나 고품질의 서비스를 제공 받을 수 있는 새로운 개념의 컴퓨팅 환경이다. 하지만 현재 클라우드 서비스 이용을 위한 ID관리 시스템은 사용자가 제공하는 개인정보를 스스로 관리/제어할 수 있는 권한을 제공하지 못하기 때문에 개인정보의 오남용이나 개인정보의 유출로 인한 프라이버시 침해 문제가 발생할 수 있다.

따라서, 본 논문에서는 이와 같은 문제를 해결하면서 보안성을 제공하기 위해 기존의 ID관리 기술 중 OpenID 방식을 확장한 사용자 중심의 새로운 ID관리 기술을 제안하였다.

현재 클라우드 컴퓨팅에 대한 표준화가 이루어지지 않아 각 서비스마다 다른 사용자 인증방식을 사용하기 때문에 상호 정보 교환이 불가능하다. 하지만 제안된 모델을 적용할 경우, 현재 개별적으로 서비스되고 있는 클라우드 서비스간의 호환성을 보장할 수 있기 때문에 서비스간 상호 정보 교환이 자유로울 것으로 예상되며, 사용자에게 자신의 개인정보를 관리할 수 있는 권한을 줌으로써 개인정보의 도용 및 프라이버시 침해 문제에 대처할 수 있을 것으로 기대된다.

참고문헌

[1] Juniper Networks, "*Identity Federation in a hybrid cloud computing environment solution guide*", JuniperNetworks, pp.1-6. 2009

[2] 민옥기,김학영,남궁한, "*클라우드 컴퓨팅 기술 동향*", 전자통신동향분석, 제24권, 제4호, pp.1-13, 2009

[3] 정제호, "클라우드 컴퓨팅의 현재와 미래, 그리고 시장전략" 한국소프트웨어진흥원, pp.56-85, 2008.

[4] Rich Maggiani, "*Cloud Computing Is Changing How We Communicate*" Professional Communication Conference, pp.1-4, 2009.

[5] John Viega, "*Cloud Computing and the Common Man*" IEEE Computer Society, Volume 42, pp. 106-108, 2009.

[6] 김동희,최진탁,"Single Sign-On 기반의 효율적인 인증 관리 기법에 관한 연구" *한국정보기술학회논문지*, 제4권, 제3호, pp.55-63, 2006.

[7] 조상래,진승헌 "사용자 중심의 ID 관리를 위한 디지털 ID 공유 프레임워크", *전자통신동향분석*, 제23권, 제6호, pp.102-103, 2008

[8] 조영섭,진승헌 "인터넷 ID 관리 시스템 개요 및 비교" *전자통신동향분석*, 제22권, 제3호, pp.136-140, 2007.

[9] 유인태 외 5명 "차세대 모바일 환경에 적합한 ID관리기

www.kci.go.kr

술 연구", *한국정보보호진흥원*, pp.3-28, 2008.
[10] 최대선,진승헌,정교일 "인터넷 ID 관리 서비스", *전자통신동향분석*, 제 20권, 제1호, pp.73-76, 2005.
[11] 조상엽, "경제 사회 시스템 보호를 위한 정보보안 정책 및 대응방안 수립", *한국지식정보기술학회 논문지*, 제4권 제1호, pp.11-19, 2009.

황문영(Moon-Young Hwang)
2008년 8월 순천향대학교 정보보호학과 졸업
2010년 1월 현재 : 순천향대학교 정보보호학과 석사과정
※ 관심분야 : 클라우드 컴퓨팅, ID 관리

곽 진(Kwak Jin)
성균관대학교 학사, 석사, 박사
2006년 4월～2006년 11월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월～2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년～2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월~현재 : 순천향대학교 정보보호학과 교수
※ 관심분야 : 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 정보보호제품 평가, 클라우드 컴퓨팅

www.kci.go.kr