Journal of the Korea Academia-Industrial cooperation Society
Vol. 12, No. 5 pp. 2353-2359, 2011

DOI: 10.5762/KAIS.2011.12.5.2353

클라우드 컴퓨팅 환경에서 효과적인 사용자 인증 프로토콜

문정경[1], 김진묵[2*], 김황래[1]
[1]공주대학교 컴퓨터공학부
[2]선문대학교 IT교육학부

An efficient user authentication protocol for cloud computing environments

Jeong-Kyung Moon[1], Jin-Mook Kim[2*] and Hwang-Rae Kim[1]
[1]**Division of Information Communication, KongJu University**
[2]**Division of Information Technology Education, SunMoon University**

요 약 최근 그린 IT의 요구와 컴퓨터 자원에 대한 효과적인 사용요구가 증가되면서 클라우드 컴퓨팅에 대한 필요성이 날로 증가되어 가고 있다. 2009년 버클리 대학에서는 클라우드 컴퓨팅을 위협하는 10대 요소를 발표하였으며 그 중에서 보안과 관련된 사용자 인증에 대한 문제가 가장 시급하게 해결되어야만 한다. 이에 본 논문에서는 클라우드 컴퓨팅 환경에서 효과적인 사용자 인증 프로토콜을 제안하고자 한다. 기존의 대표적인 사용자 인증 기법인 커베로스의 티켓 발행을 통해 사용자 인증에 대한 안전성을 보장하고, PKI의 사용자 인증을 통해 사용자 인증과 서비스 인증을 거치는 두 단계의 인증 처리 절차를 정의하였다. 제안한 인증 프로토콜에 대한 효율성과 안전성에 대한 검토 결과, 기존의 PKI 보다 구조적으로 복잡하지 않고 커베로스 보다 수행절차 및 시스템 구성을 간소화하여 응답시간을 줄였다.

Abstract The request of Green-IT technology and recommend of computer hardware resource are increasing explosively. So, necessity of Cloud computing is increasing rapidly. Berkeley Univ. announced teens constituent that threat Cloud computing in 2009 and problem for user authentication should be solved as is urgentest among them. So, We wish to propose effective user authentication protocol in Cloud computing environment. Secure safety for user quotation through Kerberos's ticket issue that is existent representative user authentication techniques, and defined authentication procedure of two steps that flow user authentication and service authentication through PKI's. Is uncomplicated structurally more than efficiency for certification protocol and examination result about safety, existent PKI that propose and simplify achievement procedure and system configuration more than Kerberos and reduced response time.

Key Words : Authentication, Certification, Cloud computing, Kerberos algorithm, PKI

1. 서론

미국의 조사기관인 가트너(Garthner)에서는 클라우드 컴퓨팅이란, '인터넷 기술을 활용하여 가상화된 IT자원을 서비스로 제공하는 컴퓨팅'으로 정의하고 있다. 클라우드 컴퓨팅의 주요 특징은 IT자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 사용한 만큼의 비용을 지불하는 것이다[1].

클라우드 컴퓨팅의 서비스 종류에 따라 3가지로 구분해 보면 표 1과 같다[2].

국내·외 클라우드 컴퓨팅 현황에 대해서 살펴보면, 국외에서는 최초로 클라우드 컴퓨팅을 제안한 구글을 시작으로 아마존, 마이크로소프트, 오라클, IBM, 야후, 최근 3par를 인수한 HP 등이 높은 관심을 보이고 있다.

*교신저자 : 김진묵(calf0425@sunmoon.ac.kr)
접수일 11년 03월 10일 수정일 (1차 11년 04월 09일, 2차 11년 04월 23일) 게재확정일 11년 05월 12일

[표 1] 클라우드컴퓨팅 모델 구분

구분	특징	사례
SaaS	소프트웨어를 사용자가 인터넷 상에서 활용하는 모델 [3][4][5]	Salesforce.com 구글 DOCS[6]
PaaS	개발자에게 소프트웨어 개발할 수 있는 토대를 마련해주는 모델	구글 Appengine [7][8]
IaaS	저장장치 또는 컴퓨팅 능력을 대여해 주는 모델	아마존 AWS [9][10][11]

국내 현황은 시장 진출 초기상태로 원천 기술이 부족한 실정이다. 2009년 12월 정부차원에서 마련한 “클라우드 컴퓨팅 활성화 종합 계획”을 중심으로 공공 클라우드 원천기술 개발, 전문인력 양성, 법 제도 정비 등이 진행이 필요하며, 2014년까지 국내 클라우드 컴퓨팅 시장을 2조 5000억 원 규모로 육성한다고 밝혔다[12].

2. 기존연구

2.1 클라우드 컴퓨팅 위협요소

지난 2009년 버클리 대학의 RAD Lab.에서 발표한 자료에 따르면 클라우드 컴퓨팅 환경을 위협하는 요소 10가지를 제시하였다. 표 2에 이를 나타내고 있다.

[표 2] 클라우드 컴퓨팅 위협요소

구분
1. Availability of Service
2. Data Lock-In
3. Data Confidentiality and Auditability
4. Data Transfer Bottlenecks
5. Performance Unpredictability
6. Scalable Storage
7. Bugs in Large Distributed System
8. Scaling Quickly
9. Reputation Fate Sharing
10. Software Licensing

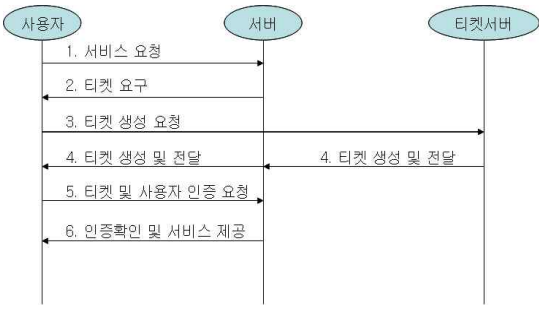
본 논문에서는 앞서 설명한 클라우드 컴퓨팅 환경에서 발생 가능한 10가지 위협 요소 중에서도 가장 시급한 인증 문제를 해결하고자 한다. 이를 위해서 기존의 대표적인 사용자 인증 기법인 커베로스와 PKI의 장점만을 적용하여 가볍고 안전하면서 클라우드 환경에 적합한 사용자 인증 기법을 제안하고자 한다.

2.2 대표적인 기존의 인증시스템

2.2.1 커베로스(Kerberos)

커베로스는 개방된 네트워크에서 사용자의 요구에 대한 인증을 위해서 최초로 제안된 인증 프로토콜이다. 이는 미국 MIT의 Athena 프로젝트에서 사용자의 서비스 요구에 대해 서버에서 사용자인증을 위해서 개발되었다.

커베로스는 사용자 인증을 위해서 암호화된 티켓(Ticket)을 사용해 사용자 서비스 요청을 검증 한다. 그림 1은 커베로스를 나타내었다.



[그림 1] 커베로스 개념 소개

2.2.2 PKI

공개키 기반구조(PKI: Public Key Infrastructure)는 공개키 암호화 방식을 사용해서 제 3 의 신뢰 기관인 CA를 중심으로 사용자에 대해 인증을 제공하는 대표적인 서비스 기반 구조이다. 이를 그림 2에 나타내고 있다.

[그림 2] PKI 개념

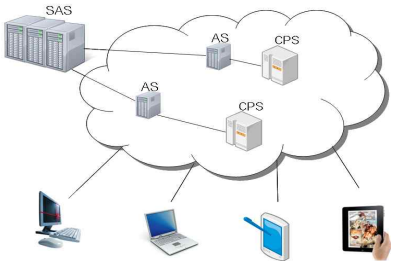
3. 제안 인증프로토콜

3.1 제안시스템 구조

전통적으로 네트워크 환경에 대한 사용자 인증을 위한 대표적인 두 가지 기법은 커베로스와 PKI 기반구조이다. 하지만 현실적으로 클라우드 컴퓨팅 환경에서는 수시로 시스템의 구성이 동적으로 바뀔 수 있는 점을 감안할 때,

기존에 사용하던 PKI 기반구조를 바탕으로 공개 클라우드 컴퓨팅 환경을 구성하는데 어려움이 있다. 추가로 커베로스 시스템도 고정된 인증서버와 티켓 발행서버, 서비스 제공 서버로 구성된 3개의 서버가 반드시 필요한데 이를 좀 더 간소화할 필요가 있다.

이에 본 논문에서는 기존의 커베로스나 PKI 구조의 장점만을 선택적으로 적용할 수 있는 새로운 인증프로토콜을 제안하고자 한다.



[그림 3] 제안 시스템 구조

그림 3과 같이 제안시스템은 사용자들이 유·무선 단말장치를 사용하여 클라우드에 자유롭게 접근이 가능하다. 그리고 사용자가 요청하는 서비스를 제공하고 관리하는 서비스 제공 시스템(CPS: Cloud-service Provide Server)이 클라우드 내부에 존재한다.

사용자의 서비스 요구에 대한 사용자 인증을 위해서 자유롭게 사용자를 관리하는 사용자 인증서버(AS: Authentication Server)는 클라우드 내부에 존재하고 사용자 인증 서버들을 구조적으로 상위 계층에서 관리하는 슈퍼 인증 서버(SAS: Super Authentication Server)가 클라우드 외부에 제 3 의 신뢰기관에서 운영하고 있음을 가정한다. 본 논문에서 사용하는 용어들을 표 3으로 정리하였다.

[표 3] 용어표

구분	설명
ID, PW	사용자 계정과 암호
#	넘버(숫자열)
RND	임의의 난수
M	메시지(Message)
TS	타임스탬프(Time Stamp)
OTP	임시 패스워드(One Time Password)
AS	Authentication Server
SAS	Super Authentication Server
CPS	Cloud-service Provide Server
Enkey[M]	key를 사용해 M을 암호화 함
Dekey[M]	key를 사용해 M을 복호화 함
s_key	비밀키, 대칭키 암호 알고리즘에 사용하는 공유된 키
h(M)	해쉬 알고리즘을 사용해 M에 대한 해쉬값을 구함
{a‖b}	a와 b 라는 자료를 연속적으로 조합
Pu_key	공개키
Pr_key	개인키
service#	사용자가 요청한 서비스 번호
,(콤마)	각각의 데이터를 구분하는 기호
Req_AN	서비스 요청 확인 번호

3.2 제안시스템 동작절차

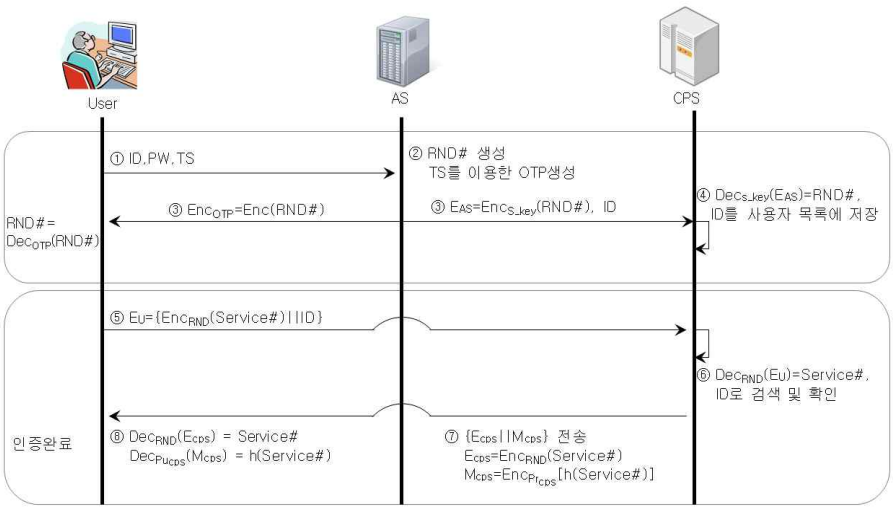
3.2.1 초기 사용자 등록 및 인증과정

본 논문에서 제안한 시스템이 동작함에 있어 2 가지 전제 조건을 갖는다.

1) 제안시스템은 초기 사용자 등록 및 인증절차와 실제 자신의 신분 인증 및 메시지 인증을 수행할 수 있다.
2) 제안시스템은 공개키 암호 알고리즘을 사용하여 사용자 인증을 수행한다.

본 논문에서 제안한 사용자 인증 시스템의 초기 사용자 인증절차는 그림 4와 같다.

1) 초기에 사용자는 AS에 사용자 등록을 수행하였음을 가정하고, ID와 PW, TS를 생성하여 전달한다.
2) AS는 사용자 정보와 TS를 사용하여 임시로 사용할 난수 RND#와 비밀키(OTP, S_Key)를 생성한다.
3) AS는 사용자에게 OTP를 비밀키로 사용하여 RND#를 암호화해 전송하고, CPS에게 E_{AS}와 ID를 비밀키로 암호화하여 전송한다.
4) CPS는 이를 복호화하여 RND#와 사용자 ID 를 목록에 저장해 둔다. 이는 차후 사용자의 서비스 요청이 발생하였을 때 사용자 인증을 수행하기 위한 것이다.
5) 사용자 서비스 요청시 요구하는 서비스 번호(Service#)를 RND#를 사용해 암호화 한 값과 사용자 계정(ID)을 조합한 E_U를 CPS에게 전송한다.
6) 사용자가 전송한 E_U를 사용자 목록에서 ID에 대한 RND#를 복호하하여 서비스요청 번호를 확인한다.
7) CPS가 복호화 한 E_U를 사용해 사용자 인증을 수행



[그림 4] 초기 사용자 인증절차

하고, 서비스 요청에 대해 RND#로 암호화 한 E_{cps}와 서비스 요청번호에 대한 해쉬값을 생성해 CPS 고유의 개인키로 암호화함으로써 전자서명과 동일한 유사한 M_{cps}를 생성해 사용자에게 응답한다.

8) 서비스 제공 시스템에 대한 인증 및 메시지 인증 : 사용자는 CPS가 보내온 E_{cps}를 복호화 하여 CPS에 대한 신분 인증을 확인하고, 사용자 자신이 전송하였던 메시지 인증 해쉬값에 대해서 복호화 해 기존에 보냈던 해쉬값과 동일성 여부를 확인해 메시지 자체를 위·변조하지 않았음을 확인한다.

제안한 인증 프로토콜에서는 초기 사용자 인증 절차를 통해서 자신의 신분 인증 및 메시지 인증을 수행할 수 있다.

3.2.2 서비스요청 및 신분 및 메시지 인증

제안시스템에서 사용자가 초기 사용자 인증절차를 만족하고 실제 서비스를 요청하는 경우에도 추가적으로 서비스를 제공하는 CPS에서 사용자의 서비스 요구에 대한 메시지 인증을 수행하게 된다.

사용자가 CPS에게 자신이 원하는 서비스를 요청하고자 서비스 요청 전송에 대한 처리절차를 그림 5에 15단계로 나타내었다.

1) 사용자 서비스 요청 : 사용자가 서비스 요청 번호, 타임스탬프를 난수로 서명한 후 타임스탬프와 조합하여 전송한다.

2, 3) User와 CPS 사이의 인증요청 : AS가 E_U를 검증하여 사용자 확인 및 CPS에게 서비스요청 번호와 ID를 CPS의 공개키로 서명해 전송한다. 추가로 AS로부터 전송되는 정보에 대한 메시지 인증 및 부인봉쇄를 위해서 AS의 개인키로 서명해서 전송한다.

4) 사용자 서비스요청에 대한 인증 확인: CPS는 수신한 사용자 서비스요청(E_{AS})에 대해서 CPS의 개인키로 검증하여 서비스요청을 확인하고, 확인한 내용에 대한 해쉬값(M_{AS})를 AS의 공개키로 검증하여 서비스 요청에 대한 인증을 확인한다.

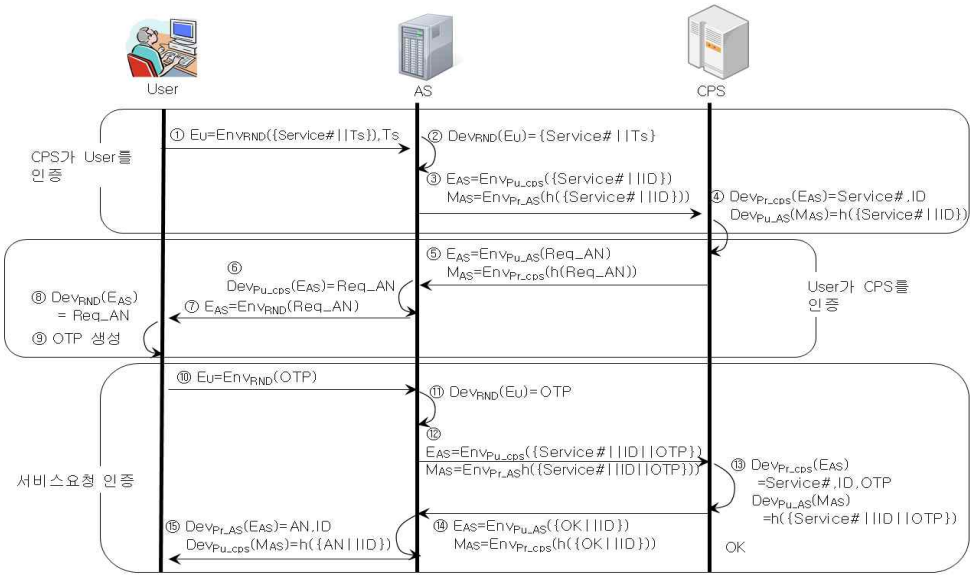
5) 서비스요청 인증 및 전송 : CPS가 사용자가 요청한 정보에 대해서 인증 확인번호(Req_AN)를 AS의 공개키로 서명한 값(E_{AS})과 Req_AN의 해쉬값을 AS의 공개키로 서명한 값(M_{AS})을 함께 전송한다. 이를 통해 부인봉쇄 및 무결성이 보장된다.

6, 7) CPS의 User 인증확인 응답 : AS가 CPS로부터 수신한 Req_AN을 CPS의 공개키로 검증해 동일성을 확인하고, 사용자에게 RND로 서명해 Req_AN을 전송한다. 이를 통해서 가로채기 공격을 막을 수 있다.

8, 9) 서비스요청 사실 확인 및 OTP 생성 : 사용자는 서비스요청 사실에 대한 CPS의 인증 여부를 확인하고, OTP를 생성한다.

10) 서비스 요청을 위한 OTP 전송 : 초기 생성된 RND로 서명하여 AS에게 OTP를 전달한다.

11, 12) 요청서비스 전달 : AS는 OTP를 확인하고, E_{AS}(Service#, ID, OTP를 CPS의 공개키로 서명한 값)와 M_{AS}(Service#, ID, OTP의 해쉬값을 AS의 개인키로 서명한 값)를 전달한다.



[그림 5] 서비스 인증절차

13) 요청서비스 확인 : CPS가 E_{AS}를 검증해 얻은 Service#, ID, OTP값을 사용해서 새롭게 만든 해쉬값(H')과 M_{AS}를 검증한 해쉬값(H)이 동일한 경우에만 서비스요청에 대한 인증을 보장한다.

14, 15) OK를 수신한 AS는 이를 서명하여 사용자에게 전송하고, 사용자는 서비스요청에 대한 사용자 인증 과정과 데이터 전달 사실에 대한 인증을 최종적으로 성공하였음을 확인한다.

4. 제안시스템 실험 및 평가

제안시스템에 대해 공개 클라우드 환경을 가정한 실험 환경을 설정하고, 시뮬레이션 결과를 살펴본다. 논문에서 수행하고자 하는 시뮬레이션에 대한 몇 가지 가정 조건은 다음과 같다.

1) 공개 클라우드 환경을 가정한다.
2) 2개의 라우팅 그룹만으로 구성하였다.
3) 각각의 서브 네트워크 환경에는 3~5대 이내로 구성된 User를 갖는다.
4) AS와 CPS는 제안 환경에서 1대씩만 존재한다.

제안 시스템의 효율성을 측정해 보고자 공개 클라우드 환경과 서버-클라이언트 환경을 구성하고 응답시간을 측정하는 시뮬레이션을 실시하였다. 이에 대한 결과를 표 4에 나타내었다.

[표 4] 클라우드 환경에 대한 응답시간

구분	공개 클라우드	서버 클라이언트
단일 노드	10 ms	10 ms
3개 노드	14.7 ms	16.4 ms
5개 노드	16.1 ms	22.6 ms

위와 같이 서브 네트워크 내에 단일 노드인 경우에는 서버-클라이언트 환경과 처리 시간이 동일하였다. 이는 공개 클라우드 환경에서 초기 지연시간이 발생하기 때문이다. 하지만, 서브 네트워크의 사용자 수가 증가할수록 응답 지연시간이 좀 더 줄어들고 있음을 알 수 있다.

본 시뮬레이션에서는 단순히 응답시간만을 측정하였다. 하지만 향후 연구에서는 보다 큰 규모의 클라우드 컴퓨팅 환경을 구성하고, 효율성 및 사용자 편의성을 측정할 수 있는 시뮬레이션을 실시하고자 한다.

본 논문에서 제안한 효과적인 클라우드 컴퓨팅 사용자 및 서비스 인증 프로토콜은 설계를 마치고 이를 시뮬레이션 하였다. 그리고 기존의 인증기법들과 제안 프로토콜에 대해 표 5에 비교하였다.

[표 5] 제안시스템 성능 비교

구분	커베로스	PKI	제안시스템
사용자인증	대칭키 기반	공개키 기반	하이브리드
메시지인증	불가능	가능	가능
사용자편의성	보통	보통	편리
효율성	빠름	느림	보통

제안한 인증 프로토콜은 커베로스와 비교해 볼 때, 상대적으로 사전 처리 단계를 필요로 하기 때문에 초기 동작 지연시간이 발생한다. 하지만 전체 동작시간에 미치는 영향은 작은 것으로 나타났다.

제안 프로토콜에 대한 안전성은 기존의 커베로스를 기반으로 하여 사용자 인증을 위한 토큰인 RND#를 생성해 OTP로 암호화하여 사용자에게 전달함으로써 중간자공격에 대해서도 안전을 보장할 수 있다. 추가로 제안한 인증 프로토콜은 실질적인 서비스를 제공하는 CPS와 독립적으로 AS가 RND와 OTP를 생성하여 인증 서비스를 제공함으로써 안전성을 보장한다.

5. 결론

클라우드 컴퓨팅은 이용 편리성이 높고 산업적 파급효과가 커서 차세대 인터넷 서비스로 주목받고 있다. 하지만, 아무리 편리하고 산업적 기대효과가 높다하더라도 보안 서비스 문제가 선결되지 않으면 무용지물이다.

본 논문에서는 클라우드 컴퓨팅 환경에서 사용자가 원하는 서비스에 대한 접근제어 및 사용자 인증, 메시지 무결성을 해결할 수 있도록 기존의 커베로스와 PKI의 단점들을 파악하고, 이를 해결할 수 있는 새로운 사용자 및 서비스 인증 프로토콜을 제안하고 세부 동작절차에 대해서 설명하였다.

제안한 인증 프로토콜은 기존의 커베로스나 PKI와 비교해 볼 때 혼용 암호화 방식을 기반으로 해 부인봉쇄 및 중간자 공격을 막을 수 있고, 사용자와 서비스 요청에 대한 상호인증 서비스도 제공할 수 있다.

향후 본 논문에서 제안한 클라우드 컴퓨팅 환경에서 효과적인 인증 프로토콜에 대해서 공개 클라우드 환경에서 보다 다양한 시뮬레이션과 새로운 기법을 적용한 인증 서비스를 제공할 수 있는 연구를 수행할 계획이다.

참고문헌

[1] 은성경 외3, 전자통신동향분석 제24권 제4호 2009. 8.

[2]http://mbn.mk.co.kr/tv/programVodList.php?programCode=474, 클라우드 컴퓨팅, 제2의 디지털 혁명 오나, 서울여대 박춘식

[3] Dave Thomas, "Enabling Application Agility-Software as a Service, Cloud Computing and Dynamic Languages," journal of Object Technology, Vol. 7, No.4, May-June 2008.

[4] 세일즈포스닷컴. "Salesforce 마케팅," http://sales-force.com

[5] KIPA, "SaaS 대표주자, Salesforce.com의 성장세 분석," 2007. 11.

[6] 정보통신동향분석 제24권 제4호 2009. 8. 클라우드 컴퓨팅 기술 동향 민옥기 외.

[7] George Lawton, :Developing Software Online with Platform-as-a-Service Technology," Computer, June 2008.

[8] Amazon, "Amazon Web Service: Overview of Security Process," http://aws.amazon.com, white paper, Sep. 2008.

[9] Michael Armbrust 외 10인, "Above the Clouds: A Berkley View of Cloud Computing," http://radlab.cs.berkeley.edu, Feb. 2009.

[10] "Amazon Elastic Compute Cloud(Amazon EC2)," http://aws.amazon.com/ec2

[11] "Amazon Simple Storage Service(Amazon S3)," http://aws.amazon.com/s3

[12] http://www.digieco.co.kr/KTFront/report/report_focus_view.action?gubun2=k&board_seq=4116&board_id=focusD&reply_group=4091&spare=k&temp_etc1=2010&temp_etc2=07 모바일 클라우드 서비스 국내외 정책 추진 현황, 이정아, 2010. 10.

[13] Joel Kirch, "Virtual Machine Security Guidelines", The Center for Internet Security, September 2007.

[14] Joel Kirch, "Virtual Machine Security Guidelines", The Center for Internet Security, September 2007.

문 정 경(Jeong-Kyung Moon) [정회원]

- 2006년 2월 : 단국대학교 산업대학원 인터넷정보학과 (공학석사)
- 2010년 3월 ~ 현재 : 공주대학교 컴퓨터공학과 대학원 박사과정

<관심분야>
클라우드 컴퓨팅, 네트워크

김 진 묵(Jin-Mook Kim) [정회원]

- 2006년 2월 : 광운대학교 컴퓨터과학과 (공학박사)
- 2006년 9월 ~ 2008년 2월 : 선문대학교 컴퓨터공학부 BK21 연구교수
- 2008년 3월 ~ 현재 : 선문대학교 IT교육학부 조교수

<관심분야>
네트워크 정보보안, RFID, 센서 네트워크, 클라우드 컴퓨팅

김 황 래(Hwang-Rae Kim) [정회원]

- 1982년 9월 : 중앙대학교 전자계산학과 이학사
- 1991년 2월 : 중앙대학교 대학원 컴퓨터공학과 공학석사
- 2007년 9월 : 대전대학교 대학원 컴퓨터공학과 공학박사
- 1983년 3월 ~ 1994년 2월 : 한국전자통신연구원 선임연구원
- 1994년 3월 ~ 현재 : 공주대학교 컴퓨터공학부 교수

<관심분야>
네트워크, 보안, 클라우드 컴퓨팅