중소기업정보기술융합학회 논문지 제2권 제2호 pp.35~41, 2012

동적 클라우드 환경에 적합한 보안 서비스 모델 설계

정윤수[1*]
[1]목원대학교 정보통신공학과

Design of Security Service Model in Dynamic Cloud Environment

Yoon-Su Jeong[1*]
[1]Department of Information Communication Engineering, Mokwon University

요 약 최근 클라우드 컴퓨팅과 모바일 인터넷 서비스의 급속한 발전은 사용자가 언제 어디서나 인터넷을 통하여 원하는 컴퓨팅 자원을 제공받고 지불하는 모바일 클라우드 서비스 환경으로 변화하고 있다. 그러나 모바일 클라우드 환경에서 사용자가 사용하는 모바일 기기를 사용자가 분실하였을 경우 사용자의 정보유출 및 외부에 위탁한 정보에 대한 접근통제 우회 등의 보안 위협에 대한 대응방법이 미흡한 실정이다. 본 논문에서는 모바일 클라우드 사용자가 서로 다른 레벨의 다른 사용자에게 안전하게 서비스를 제공하기 위한 클라우드 서비스 접근 제어 모델을 제안한다. 제안 모델은 다양한 접근 보안 정책을 적용할 수 있도록 사용자 및 단말이 인증을 수행할 때 역할기반의 접근권한 관리를 수행한다. 또한, 제안된 모델은 사용자의 속성 정보를 이용하여 사용자 인증 과정 전에 처리하기 때문에 통신 오버헤드 및 서비스 지연을 낮추고 있다. 실험 결과, 제안 모델이 기존 모델보다 패킷 인증 지연시간은 평균 3.7% 향상되었고, 인증서버의 처리량은 평균 10.5% 향상된 결과를 얻을 수 있었다.

키워드 : 동적 클라우드, 보안 서비스, 사용자 인증

Abstract The rapid development of cloud computing and mobile internet service changes to an mobile cloud service environment that can serve and pay computing source that users want anywhere and anytime. But when user misses mobile device, the respond to any threat like user's personal information exposal is insufficient. This paper proposes cloud service access control model to provide secure service for mobile cloud users to other level users. The proposed role-based model performs access authority when performs user certification to adapt various access security policy. Also, the proposed model uses user's attribute information and processes before user certification therefore it lowers communication overhead and service delay. As a result, packet certification delay time is increased 3.7% and throughput of certification server is increased 10.5%.

Key Words : Dynamic Cloud, Security Service, User Authentication

1. 서론

최근 정보화 사회가 진행됨에 따라 스마트폰, 테블릿 PC 등 다양한 모바일 기기를 사용하여 기업의 영업 파일 및 개인의 민감한 데이터 파일을 정확하고(무결성) 안전하게(기밀성) 관리하는 기술의 중요성이 부각되고 있다. 특히, 모바일 클라우드 컴퓨팅은 이러한 사회적 요구사항을 반영하여 인터넷 기술과 모바일 통신 기반의 가상화된 IT 자원을 서비스로 제공하고 있으며 개인 PC나 기업의 서버에 개별적으로 저장해 두었던 프로그램이나 문

이 논문은 2012년 중소기업정보기술융합학회 추계학술발표대회의 우수논문을 확장한 것임.
*교신저자(e-mail: bukmunro@mokwon.ac.kr)
접수일(2012년 11월 15일), 심사완료일(2012년 11월 30일)

서를 모바일 기기를 이용하여 사용한다[1,2].

모바일 클라우드 컴퓨팅은 모바일 기기의 이동성에 대한 특성으로 인하여 IT 자산을 타 사용자와 쉽게 공유하지만 클라우드 컴퓨팅이 제공하는 서비스 구조가 서로 다르기 때문에 데이터의 무결성 및 서버의 인증 문제에 대한 보안위협에 대한 취약점이 존재한다[3].

모바일 클라우드 컴퓨팅은 기존 클라우드 컴퓨팅 환경에서 제공되는 자원의 레벨에 따라 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service) 모델로 클라우드 서비스가 분류되며, 클라우드 서비스 특성에 따라 가상화, 자원공유 및 집중화, 정보위탁, 단말의 다양성 등으로 분류되어 서비스되고 있다.

모바일 클라우드 컴퓨팅에서는 이동 사용자가 클라우드 컴퓨팅 서버로부터 필요한 자원의 일부 또는 전부를 직접 공급받기 위해서 서버는 클라우드 서비스의 인증 시스템을 활용하여 이동 사용자를 인증하고 있다. 또한, 모바일 클라우드 컴퓨팅은 이동 사용자가 자신의 환경을 간편하게 구성하고 수시로 변경이 가능하다.

본 논문에서는 모바일 클라우드 사용자가 서로 다른 레벨의 클라우드 보안 서비스를 서로 다른 사용자에게 안전하게 제공하기 위한 클라우드 서비스 접근 제어 모델을 제안한다. 제안 모델은 사용자 및 단말이 인증을 수행할 때 다양한 접근 보안 정책을 적용할 수 있도록 사전에 역할기반의 접근권한 관리를 수행한다. 또한, 제안 모델은 사용자의 속성 정보를 이용하여 사용자 인증 전에 처리하기 때문에 통신 오버헤드 및 서비스 지연과 같은 통신 장애를 최소화할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 모바일 클라우드 개념 및 보안 이슈에 대해서 설명한다. 3장에서는 역할기반 접근통제와 사용자 속성정보를 이용한 모바일 클라우드 보안 서비스 모델을 제시하고, 4장에서는 제안 모델에 대한 성능평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련연구

2.1 클라우드 컴퓨팅의 개념

클라우드 컴퓨팅은 그림 1과 같이 정보가 인터넷 상의 서버에 영구적으로 저장되고, 데스크톱, 태블릿 컴퓨터, 노트북, 넷북, 스마트폰 등의 IT 기기 등과 같은 클라이언트에 일시적으로 보관되는 컴퓨팅 서비스를 의미한다[1,2].

클라우드 컴퓨팅에서는 기업 또는 개인이 컴퓨터 시스템을 유지·보수·관리하기 위해서 들어가는 비용과 서버의 구매 및 설치 비용, 업데이트 비용, 소프트웨어 구매 비용 등 엄청난 비용과 시간·인력을 줄일 수 있고, 에너지 절감에도 기여할 수 있는 장점이 있다.

또 PC에 자료를 보관할 경우 하드디스크 장애 등으로 인하여 자료가 손실될 수도 있지만 클라우드 컴퓨팅 환경에서는 외부 서버에 자료들이 저장되기 때문에 안전하

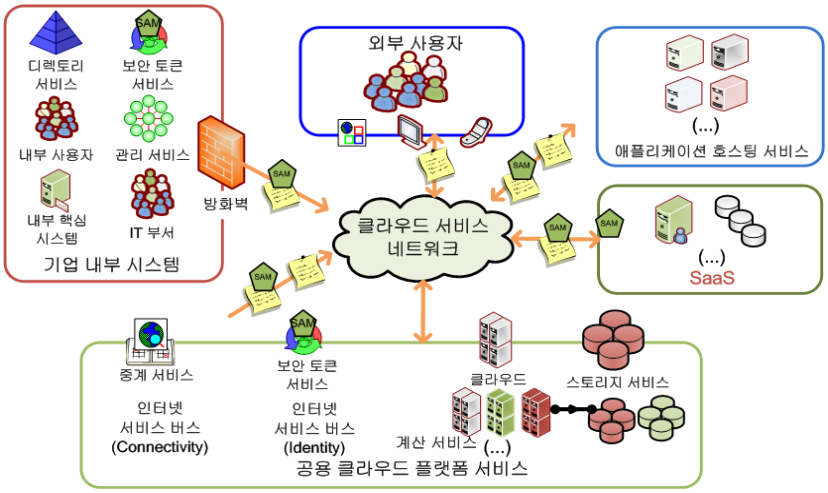

그림 1. 클라우드 개념
Fig 1. Cloud Concept

게 자료를 보관할 수 있고, 저장 공간의 제약도 극복할 수 있으며, 언제 어디서든 자신이 작업한 문서 등을 열람·수정할 수 있다. 하지만 서버가 해킹당할 경우 개인정보가 유출될 수 있고, 서버 장애가 발생하면 자료 이용이 불가능하다는 단점도 있다.

클라우드 컴퓨팅 환경을 구축하기 위하여 가장 기본이 되는 가상화 기술은 한 대의 물리적인 장비 중에서 현재 사용되지 않는 부분을 마치 다른 장비 한 대가 추가된 것처럼 인식시켜 업무를 수행하거나 여러 대의 장비를 잠시 동안 연결시켜 고성능, 고용량 장비처럼 활용할 수도 있다[2].

2.2 모바일 클라우드

모바일 클라우드는 그림 2와 같이 기존 클라우드 컴퓨팅에서 사용자의 이동성을 제공하는 서비스 형태로써 클라우드 컴퓨팅의 편리성과 확장성을 기반으로 다양한 플랫폼 및 운영체제를 제공하는 시스템이다.

2012년 현재 전 세계적으로 모바일 클라우드 서비스가 지속적으로 구축되고 있으며, 국내에서도 정부와 공공기관 그리고 산업계를 중심으로 다양한 형태의 모바일 클라우드 서비스가 구축되고 있다.

최근 모바일 클라우드 서비스 연구에서는 클라우드 센터의 위치문제, 서비스 안정화, 보안, 개인정보 보호, 내부 클라우드 내부 운용성, 소프트웨어 라이선스 및 지적재산권, 정보 및 IT Compliance 등 다양한 쟁점들에 대한 연구가 지속되고 있다.

모바일 클라우드 컴퓨팅은 모바일 응용서비스 개발자와 모바일 단말 사용자에게 서버 기반의 클라우드 컴퓨팅 서비스를 제공하고 모바일 단말들로 구성된 클라우드에서 정보와 자원을 공유하는 서비스를 의미한다[1].

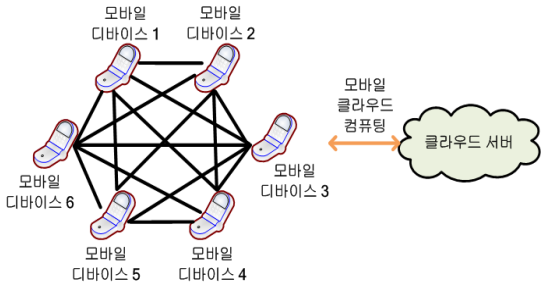

그림 2. 모바일 클라우드 구성도
Fig 2. Structure of Mobile Cloud

2.3 모바일 클라우드 특성

모바일 클라우드는 모바일 단말-클라우드 서비스 제공자 간 클라우드 제공과 모바일 단말-단말 간 클라우드를 제공의 2가지 특징을 가진다. 모바일 단말-클라우드 서비스 제공자간 클라우드 서비스를 제공은 기존의 클라우드 서비스가 모바일 단말에 심리스하게 서비스를 제공하며, 모바일 단말-단말 간 클라우드 서비스를 제공하는 것은 모바일 단말의 자원을 연계하여 클라우드 서비스를 제공한다. [표 1]은 모바일 클라우드 특성을 서버-모바일 단말 간 클라우드와 모바일 단말-단말 간 클라우드를 세부적으로 분석한 결과이다.

3. 역할기반과 개인속성을 이용한 클라우드 보안 모델 설계

이 절에서는 스마트폰과 같은 휴대기기를 이용하여 클라우드 서버의 공유 서비스를 이용하여 서로 다른 레

표 1. 모바일 클라우드 특성[1]
Table 1. Character of Mobile Cloud

서버-모바일 단말 간 클라우드	·단말 기종과 OS 비종속적인 모바일 응용 개발 플랫폼 제공 ·모바일 단말의 응용 실행 환경(H/W 자원, OS 유틸리티, 응용)을 하나의 인스턴스로 제공하고 사용자 인스턴스들의 이동성 및 확장성 제공 ·모바일 단말-서버간 싱크/캐쉬 기능 제공 ·모바일 클라우드 단말 및 서버 보안 기술
모바일 단말-단말 간 클라우드	·단말 간 클라우드 구성 에이전트 기술 ·자원(정보 및 HW 자원)공유를 위한 플랫폼 기술 ·단말 이동성에 따른 단말 간 클라우드 자동 재구성 기술 ·단말 간 클라우드 구성 단말의 안정성 확보 기술

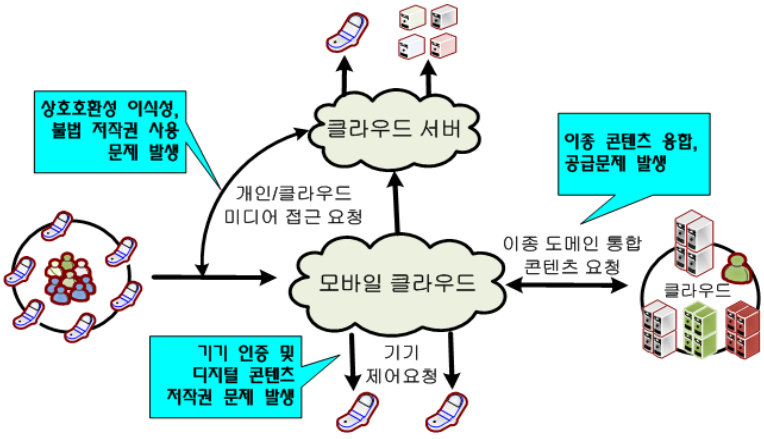

그림 3. 모바일 클라우드 환경에서의 보안 문제
Fig 3. Security Problem in Mobile Cloud Environment

벨의 클라우드 보안 서비스를 사용자들에게 안전하게 제공하기 위한 클라우드 서비스 접근 제어 모델을 제안한다.

3.1 보안 요구사항

모바일 클라우드는 [그림 3]처럼 사용자가 모바일 기기를 사용함으로써 발생되는 대표적인 보안 문제(상호호환성 이식성 및 불법 저작권 사용 문제, 이종 콘텐츠 융합 및 공급문제, 기기 인증 및 디지털 콘텐츠 저작권 문제 발생 등)에 취약하다. 상호호환성 이식성 및 불법 저작권 사용 문제에서는 사용자가 사용하는 다양한 스마트 기기와 콘텐츠들은 모바일 클라우드 환경에서 안전하게 서비스를 제공하기 위해서 콘텐츠의 유통과 공유를 개인 및 사업자간 디지털 콘텐츠의 저작권 보호가 필요하다[4,5].

이종 콘텐츠 융합 및 공급문제에서는 모바일 클라우드 환경에서 사용되는 단말들을 연계하여 컨텐츠를 제공하도록 디바이스의 접근 제어 기술이 필요하다. 모바일 환경에서 기기 인증 및 디지털 콘텐츠 저작권 문제에서는 서로 다른 기기를 사용하는 사용자를 모바일 클라우드 시스템의 인증서버에서사용자의 역할 및 권한에 따라 컨텐츠 서비스를 제한하도록 인증을 수행해야 한다.

3.2 클라우드 보안 모델 설계

제안된 클라우드 보안 서비스 모델은 [그림 4]와 같다. [그림 4]처럼 외부 사용자가 모바일 클라우드 서비스를 제공받기 위해서는 디바이스 기기와 서비스 서버 사이에 서비스 접근 보안 엔진을 통해 사용자의 권한 및 등급에 따라 서비스를 제한한다. 접근보안 엔진은 사용자 기기에 대한 신뢰성 관리자와 접근성 관리자를 통해 사용자의 개인정보 속성을 인증서버와 컨텐츠 서버 내 데이터베이스에 저장되어 있는 정보와 비교평가한 후 검증이 정상적으로 수행될 경우 사용자 레벨에 따라 컨텐츠를 제공한다. 제안 모델에서 컨텐츠를 제공하는 서버는 일정 시간동안 사용가능하도록 설정되며, 사용자를 인증하기 위해서 인증 서버에게 사용자의 인증정보를 확인하는 것이 아니라 접근 보안 엔진 내 데이터베이스에 저장되어 있는 사용자의 개인속성 정보의 인증 유·무 정보를 인증 서버를 통해 확인하는 과정을 수행한다. 이 과정을 통해 제안 모델에서는 프록시 기능을 통해 인증 서버의 오버헤드와 컨텐츠 서버의 서비스 지연을 최소화하는 효과를 얻는다.

표 2. 개인 속성 정보
Table 2. Personal Property Information

GID	*ID*	*AI*	*Time*	AIP	*GI*

제안 모델에서는 오버헤드와 서비스 지연을 최소화하기 위해서 사용자가 접근할 때마다 접근 보안 엔진의 보안 관리자를 사용자의 권한 및 신뢰 등급을 확인한다. [표 2]는 접근 보안 엔진 내 사용자의 개인 속성에 따라 인증 서버와의 동기화를 통해 사용자의 신뢰성을 평가하는 정보의 각 필드를 보여주고 있다. [표 2]에서 *GID*는

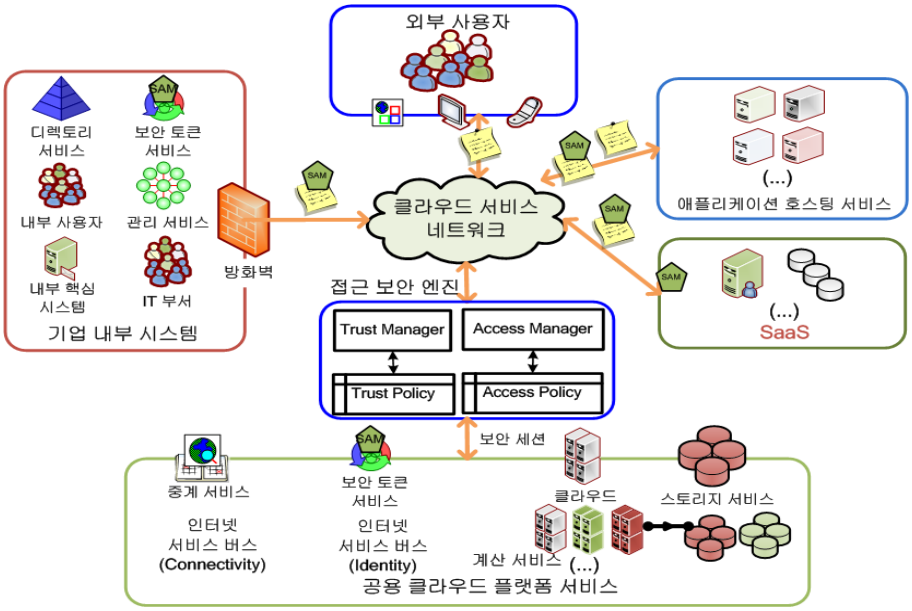

그림 4. 역할기반과 개인속성기반의 클라우드 보안 서비스 모델
Fig 4. Cloud Security Service Model based on RBAC and Personal Info.

개인 사용자가 속한 클라우드 그룹 인식자를 나타내고, *ID*는 사용자의 개인 인식자 정보를 나타낸다. *AI*는 인증서버와 동기화 유·무를 나타내는 정보로써 동기화가 정상적으로 수행되면 1, 정상적으로 수행되지 않으면 0으로 나타낸다. *Time*은 사용자가 클라우드 서비스를 요청한 시간을 나타내고, *AIP*는 사용자가 인증서버로부터 부여받은 인증 확률 비율로써, 이 값은 클라우드 환경에서 비정상적인 사용자의 접근을 제한하는 역할을 담당한다. GI는 현재 사용자가 속한 클라우드 그룹 정보로써, 사용자의 활동내역 정보를 나타낸다.

표 3. 접근 관리 보안정보
Table 3. Access Management Secuirty Information

ID	*Grade*	*Time*	*PI*	*DI*

[표 3]은 접근 보안 엔진내 사용자의 역할에 따라 접근을 제어하기 위해서 신뢰 관리자가 체크하는 정보의 각 필드를 나타내고 있다. *ID*는 사용자의 인식자를 나타내고 *Grade*는 사용자의 권한 등급을 나타낸다. *Time*은 사용자가 클라우드 서비스를 요청한 시간을 나타내고, *PI*는 사용자의 퍼미션 정보를 나타낸다. *DI*는 사용자 이동기기의 정보를 나타낸다.

4. 평가

4.1 환경설정

이 절에서는 모바일 클라우드 환경에서 모바일 기기를 사용하는 사용자가 공용 클라우드 플랫폼 서비스에 접근할 때 사용자의 역할과 개인속성을 통하여 사용자 인증을 수행함으로써 인증서버의 오버헤드와 컨텐츠 서버의 서비스 지연을 최소화하는 것을 기존 기법과 비교 평가한다[6].

표 4. 실험 환경
Table 4. Experimental Environment

환경 변수	값
사용자(모바일 기기) 수	1,000
동시 최대 인식수	100
실험시간	3600 s
버퍼 크기	50 packet/s
패킷 드롭 확률	0.01
데이터 패킷 크기	100 bytes
쿼리 패킷 크기	25 bytes
헤더 패킷 크기	25 bytes

[표 4]처럼 실험에서 모바일 기기를 사용하는 사용자 수는 1,000명으로 설정하며 접근 보안 엔진이 동시에 모

바일 기기를 동시에 인식할 수 있는 최대수는 100로 설정한다. 모바일 클라우드 서버는 모바일 기기로부터 데이터 패킷을 전송하고 3600초 동안 실험을 수행한다. 인증서버의 버퍼 크기는 50패킷의 크기를 가지는 것으로 가정하며, 각 패킷은 패킷 전송동안 패킷 드롭 확률을 0.01로 한다. 이 같은 설정은 현실 모델에 맞는 시뮬레이션을 만들기 위한 설정들이다.

4.2 실험결과

[그림 5]에서는 접근 보안 엔진을 통해 사용자의 서비스 요청에 따른 컨텐츠 서버의 서비스 지연시간을 제안모델과 기존모델을 비교평가하고 있다. 실험 결과, 제안모델은 사용자 속성정보와 역할기반 사용자 권한 및 등급을 인증서버에 확인할 때 프록시 기능을 통해 인증을 수행하여 사용자 인증 정보를 컨텐츠 서버에게 전달하여 사용자에게 컨텐츠 서비스를 제공하기 때문에 기존모델보다 컨텐츠 서버가 사용자에게 서비스를 제공하는 지연시간이 3.1% 향상된 결과를 나타내고 있다.

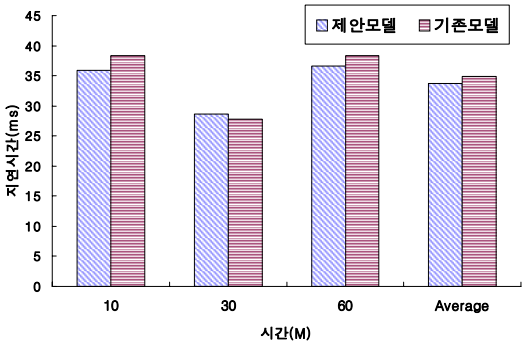

그림 5. 인증 지연시간
Fig 5. Delay Time of Authentication

[그림 6]은 모바일 기기수에 따른 인증서버의 오버헤드를 제안기법과 기존기법을 비교평가하고 있다. 실험 결과, 제안 모델은 사용자의 속성정보를 프록시하여 인증서버에게 전달하여 인증서버의 데이터베이스에 저장되어 있는 사용자 정보의 권한 및 등급을 비교하여 사용자의 안전성을 검증하기 때문에 기존모델보다 인증서버의 오버헤드가 평균 21% 낮게 나타내고 있다.

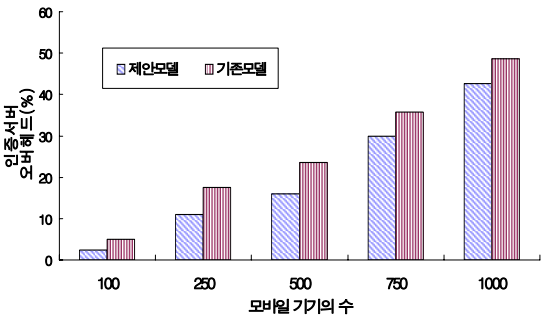

그림 6. 모바일 기기수에 따른 인증서버의 오버헤드
Fig 6. Overhead of Authentication Server through Number of Mobiile Device

5. 결론

최근 모바일 클라우드 서비스는 사용자의 이동성 따른 정보유출 및 접근통제 우회와 같은 보안 피해가 급증하고 있다. 본 논문에서는 모바일 클라우드 환경에서 사용자가 서로 다른 서비스를 안전하게 제공받는 클라우드 서비스의 접근 제어 모델을 제안하였다. 제안 모델은 다양한 접근 보안 정책을 적용할 수 있도록 공용 클라우드 플랫폼 서비스에 접근 보안 엔진을 추가하여 사용자 및 단말이 인증을 수행할 때 역할기반의 접근권한 관리를 수행하도록 하였다. 제안 모델은 사용자의 속성정보만을 프록시 형태로 인증정보에 전달하여 인증을 수행함으로써 지연시간과 오버헤드를 낮추었다. 실험 결과, 컨텐츠 서버의 서비스 지연 시간은 기존 기법보다 3.1% 향상하였고, 모바일 기기수에 따른 인증서버의 오버헤드는 21% 낮게 나타났다. 향후 연구에서는 제안된 모델을 실제 환경에 적용할 수 있도록 구현하여 성능평가를 수행할 계획이다.

참 고 문 헌

[1] 이강찬, 이승윤, “모바일 클라우드 표준화 동향 및 전략”, 한국통신학회지(정보와통신) 28권 10호, pp. 44-49, 2011.

[2] 정인안, 이창용, 김정욱, 김환국, 정현철, “모바일 클라우드 Multi-tenancy 환경에서 상황인지형 동적 인증 및 권한관리 서비스”, 정보보호학회지 21권 8호, pp. 14-22, 2011년 12월.

[3] 박완규, “클라우드 컴퓨팅 환경에서의 개인정보의 미국 이전에 따른 문제점 및 대응방안 연구”, 경북대학교 법학연구소,

법학논고 38, pp. 455-478, 2012년 2월.
[4] 정윤수, 김용태, “이중 해쉬 체인 기반의 플로딩 패킷 인증 및 무결성 보장 메커니즘”, 한국정보기술학회논문지 9권 1호, pp. 147-158, 2011년 1월.
[5] 정윤수, 김용태, “아이핀 기반의 유헬스케어 사용자 정보 보호 프로토콜”, 한국정보기술학회논문지 9(10), pp. 133-141, 2011년 10월.
[6] 장은영, 박춘식, “클라우드 컴퓨팅 서비스의 가용성 최적화를 위한 모델링 및 시뮬레이션”, 한국시뮬레이션학회논문지 20권 1호, pp. 1-8, 2011년 3월.

저 자 소 개

정 윤 수(Yoon-Su Jeong) [정회원]

- 1998년 2월: 청주대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수

<관심분야> : 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안