클라우드 시스템에서의 사용자 데이터 보호에 관한 연구

이애리[*], 조도은[**], 이재영[***]

A Study on the Protection of User Data in the Cloud System

Ae-Ri Lee[*], Do-Eun Cho[**], Jae-Young Lee[***]

요 약 클라우드 컴퓨팅은 인터넷 기술을 활용하여 IT자원을 서비스로 제공하는 컴퓨팅으로 최근 많은 관심을 받고 있다. 클라우드 스토리지 서비스들은 사용자에게 편리함을 제공하지만, 그러나 사용자 데이터에 대한 접근을 데이터 소유자가 통제하기 어렵기 때문에 데이터 기밀성을 보장하지 못하는 문제점이 있다. 본 논문에서는 클라우드 시스템에서 사용자 데이터 보호를 위하여 사용자 데이터를 블록으로 분할하여 그 중 한 블록에 대해서만 공개키 암호화 방식을 이용한 기법을 제안하였다. 따라서 클라우드 스토리지 서버에 저장된 사용자 데이터에 대한 기밀성과 무결성을 제공한다.

주제어 : 클라우드 컴퓨팅 시스템, 데이터 보호, 프라이버시, 클라우드 컴퓨팅 구조, RAID

Abstract The cloud computing is a system that provides IT resources service by using internet technologies, which grabs lots of attention today. Though cloud storage services provide service users with convenience, there is a problem in which data confidentiality is not guaranteed because it is hard for data owners to control the access to the data. This article suggested the technique by applying Public-Key Cryptosystem only to a block after dividing users' data into blocks in order to protect users' data in cloud system. Thus confidentiality and integrity are given to users' data stored in cloud storage server.

Key Words : Cloud Computing System, Data Protection, Privacy, Cloud Computing Architecture, RAID

1. 서 론

클라우드 컴퓨팅은 IT와 관련된 기능들이 서비스 형태로 제공되는 컴퓨팅 스타일로 최근 많은 관심을 받고 있다. 현재 클라우드 컴퓨팅 시장은 초기 도입기를 거치고 있으며 웹메일, 블로그, 웹하드 서비스, 웹호스팅 서비스 등이 이미 사용되고 있다. 그러나 본격적인 성장단계로 진입하기 위해서는 사용자의 요구수준에 맞는 애플리케이션과 서비스 발굴, 기존 시스템과의 연동성 확대, 보안에 대한 우려 불식 등과 같은 문제들이 선결되어야 한다[1].

클라우드 컴퓨팅의 스토리지 서비스는 일반적으로 사용자에게 높은 신뢰성과 편리함을 주는 저렴한 가격의 웹하드 서비스로 인식된다. 하지만 사용자들은 그들의 중요한 개인 데이터들을 클라우드 서버에 저장하길 꺼려한다. 이는 클라우드 서버에 저장된 자신의 데이터가 다른 사람에게 노출될 수 있다고 생각하기 때문이다. 따라서 클라우드 컴퓨팅이 널리 사용되기 위해서는 사용자의 데이터가 안전하게 보호되는 환경이 우선시 된다. 한 가지 방법으로 암호화를 기반으로 데이터를 보호하는 방법이 있다. 하지만 완벽하게 안전한 암호화 기법은 아직 존재하지 않는다. 또한 모든 데이터를 암호화를 하는데 에는 CPU 자원이 많이 소모된다. 또한 소유처가 분명한 기존 서버와 네트워크에서도 보안사고가 빈번하게 발생하는 현시점에서 수많은 사람들이 공유하여 사용하는 클라우드 컴퓨팅의 기술적 보안을 어떻게 보장할 것인가는

[*]세명대학교 컴퓨터학부 강사
[**]목원대학교 공학교육혁신센터 조교수
[***]세명대학교 교양과정부 조교수(교신저자)
논문접수: 2012년 11월 20일, 1차 수정을 거쳐, 심사완료: 2012년 12월 15일

중요한 문제이다. 이러한 이유로 현재 클라우드 컴퓨팅 기술 및 보안에 대한 연구가 활발히 진행되고 있다.

확장성과 가용성이 클라우드 컴퓨팅 서비스의 기본조건 이라면, 보안성은 이 서비스가 실질적으로 상용화됨에 있어서 가장 예민하게 개입되는 요소이다. 특히 모든 컴퓨팅 서비스가 고객과의 돈독한 신뢰를 기반으로 해서만 제공될 수 있다는 점에서 보안성의 확보는 더없이 중요하다. 데이터의 보안성이 확보되지 않는다면 클라우드 컴퓨팅 서비스는 무의미해지기 때문이다. 따라서 내외부 보안성에 대한 확실한 신뢰를 구축하는 것은 클라우드 컴퓨팅 서비스 상용화의 관건이 될 것이다[2].

일반적으로 클라우드 컴퓨팅 환경에서는 물리적 자원을 추상화하여 원하는 형태로 해당 자원을 분리·통합할 수 있게 하는 기술인 가상화 기술을 사용한다. 가상화 기술은 실제로는 한 대의 서버를 여러 대인 것처럼 나눠서 쓸 수 있고, 여러대의 서버를 한 대인 것처럼 묶어서도 사용할 수 있다.

본 논문은 클라우드 시스템 환경에서 사용자의 데이터를 블록으로 분할하여 그 중 한 블록에 대해서만 암호화하는 기법으로 사용자 데이터의 보호에 대하여 연구하였다.

본 논문의 구성은 2장에서는 클라우드 시스템과 보안성 문제에 대해 살펴보고, 3장에서는 제안된 시스템에 대하여 설명을 한다. 그리고 4장에서는 제안하는 시스템의 안전성 분석에 대하여 기술하고, 마지막 5장에서는 결론으로 마무리한다.

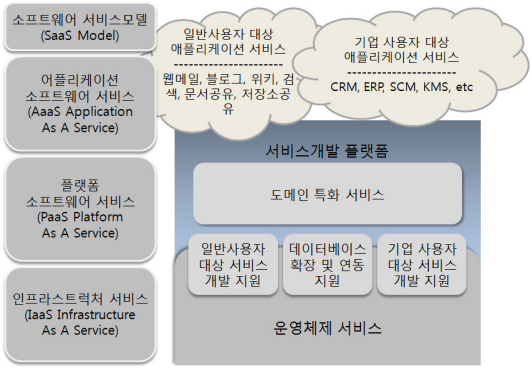
2. 관련 연구

2.1 클라우드 시스템

클라우드 컴퓨팅이란 '인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅'이다. 주요 특징으로는 IT자원을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며 사용한 만큼의 비용을 지불하는 것을 들 수 있다.

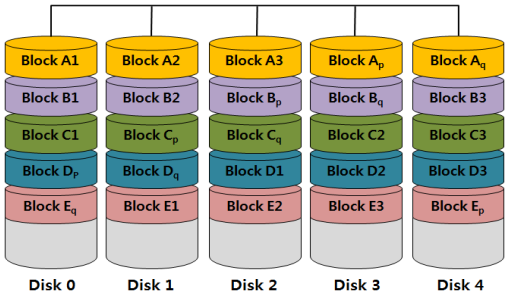
이러한 클라우드 컴퓨팅을 제공하기 위한 서비스를 분류해 보면 다음과 같다[3].

IaaS(Information as a Service)는 서버, 데스크탑 컴퓨터, 스토리지 같은 IT 하드웨어 자원을 클라우드 서비스로 빌려 쓰는 형태를 말하며, 이를 기반으로 H/W를 구성한다. PaaS(Platform as a Service)는 소프트웨어 개발자들이 자신이 원하는 소프트웨어를 구현할 수 있도록 지원하며, 이는 응용 소프트웨어를 제작하기 위한 도구인 프로그래밍 언어를 제공하는 수준을 넘어서 미들웨어까지 포괄하는 사용자 개발 플랫폼을 제공한다. SaaS(Software as a Service)는 클라우드 컴퓨팅 서비스를 사업자가 인터넷으로 소프트웨어를 제공하고, 사용자가 인터넷에 원격으로 접속해서 소프트웨어를 활용하는 모델이다. [그림 1]은 클라우드 컴퓨팅의 플랫폼과 서비스를 나타낸 것이다.



[그림 1] 클라우드 플랫폼

가상화는 컴퓨터의 운영체제로부터 물리적 하드웨어를 분리하여 IT 리소스의 활용률과 유연성을 극대화하기 위한 추상화 개념이다. 클라우드 컴퓨팅의 스토리지 서버 가상화는 RAID 어레이 구성으로 여러개의 하드 디스크를 연결하여 디스크의 속도를 빠르게 하면서도 자동으로 백업이 되게 만들어 안전성을 높인다.



[그림 2] RAID의 구성

데이터 프라이버시를 제공하기 위한 기술로는 데이터를 암호화하여 저장하는 방법이 있다. 정당한 키를 가진

사용자만이 암호화된 데이터를 복구해 볼 수 있기 때문에 키를 모르는 공격자는 저장된 암호문으로부터 그 내용에 대한 정보를 얻을 수 없어 안전성이 보장된다.

2.2 클라우드 시스템의 보안 이슈

클라우드 컴퓨팅을 통해 모든 자원이 공유되는 상황은 자원의 효율성과 비용 절감을 가져오는 것이지만, 동시에 내부의 중요한 데이터가 외부 네트워크와의 연결에서 유출되거나 노출될 위험을 안고 있는 것이기도 하다. 따라서 클라우드 컴퓨팅 서비스의 보안 문제는 고객과의 신뢰를 확보할 수 있을 만큼 안정적인 제안이 되어야 한다[4].

클라우드 컴퓨팅 보안 이슈를 구분해 보면 다음과 같다.

첫째, 개인 사용자 관점에서 살펴보는 클라우드 컴퓨팅 보안이슈이다. 현재 IT 자원 공유 시스템을 활용하는 개인 사용자들은 주로 메일이나 사진, 파일 저장 등의 서비스를 이용한다. 개인 사용자들이 가장 우려하는 보안 문제로는 민감한 개인정보의 노출 및 개인의 감시, 사적 데이터에 대한 상업적 악용을 들 수 있다.

둘째, 기업 사용자의 관점에서 살펴보는 클라우드 컴퓨팅의 보안 이슈이다. 기업 사용자는 클라우드 서비스를 이용하되 자신의 데이터가 타인과 공유되는 것을 원하지는 않는다. 또한 기업이 소유한 많은 개인 사용자들의 정보 뿐만 아니라, 외부에 유출되어서는 안되는 수많은 기밀들이 내부 서버를 통해 공유되어야 하기 때문이다. 이는 훨씬 더 엄격하고 광범위한 보안 문제라 할 수 있다.

따라서 클라우드 시스템에서의 보안 요구사항은 다음 <표 1>과 같이 정리될 수 있다[5].

개인 및 기업 데이터에 대한 기밀성 보호를 위해서는 기본적으로 암호화 기술이 제공되어야 한다. 특히 클라우드 컴퓨팅에서는 대용량 데이터의 암호화 시 전체 시스템의 가용성이 떨어질 수 있다는 점을 고려하여 이러한 상황에 적합한 암호 기법이 이용되어야 한다.

또한 클라우드 컴퓨팅에서는 저장되는 데이터와 교환되는 메시지에 대한 오류 검사가 매우 중요하다.

그리고 서비스의 중단이나 데이터의 손실을 막기 위해서는 사고 시 서비스를 지속할 수 있는 고장 감내성 및 데이터 복구 기법에 대한 연구가 매우 중요하다.

다수 사용자의 데이터가 혼재되어 있는 클라우드 환경에서는 사용자에 대한 인증과 권한 관리 기술이 더욱 필요하며, 다수의 사이트와 다수의 서비스를 통합 인증하는 SSO(Single-Sing On)형태의 인증 기술이 많이 연구 되고 있다. 따라서 클라우드 컴퓨터 환경에서 사용자에 대한 신원확인과 사용자별로 할당된 권한에 따른 접근제어 기준 보유 여부를 확인하는 것은 필수 요소라 할 수 있다 [6][7].

<표 1> 클라우드 시스템의 보안 요구사항

구분	내용
기밀성	클라우드 서비스 환경은 다수의 사용자들이 공유 환경에서 서비스를 이용하기 때문에 개인 및 기업 데이터에 대한 기밀성과 데이터 암호화가 필요함
무결성	저장되는 데이터와 교환되는 메시지에 대한 오류 및 변조 여부 확인을 위한 데이터 무결성이 요구됨
가용성	사고로 인한 서비스 중단이나 데이터 손실을 막기 위해 사고 발생시 서비스의 지속성을 위한 가용성 및 복구가 필요함
사용자 인증 및 접근제어	다수 사용자의 데이터가 혼재되어 있는 클라우드 환경에서의 사용자에 대한 인증과 권한 관리를 위한 사용자 인증 및 접근 제어가 필요함

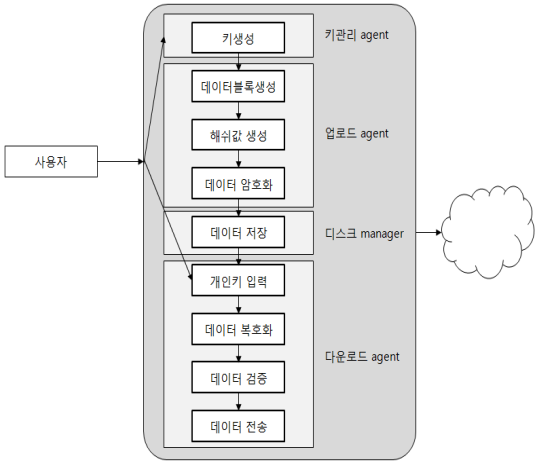
3. 제안하는 사용자 데이터 보호 기법

클라우드 서비스 사용자는 사용자 데이터를 클라우드 서비스 제공자가 제공하는 원격 데이터 서□ 제공젠장한다. 그러나 젠장된 사용자의 데이터가 서□ 의 관리자에 의해 복사, 이동, 수정될 가능성이 있으며 이러한 경터 사용자는 데이터의 변경 내역을 알아내기가 어려우며 통제가 불가능할 수도 있다[8].

이에 본 논문에서는 클라우드 데이터 서버에 저장된 사용자 데이터에 대한 접근, 복사, 이동, 수정을 막는 사용자 데이터 보호 방법에 대하여 제안한다.

가장 기본적인 데이터 보호 방법은 전체 데이터를 모두 암호화 하여 저장하는 것이다. 그러나 대용량의 데이터를 한꺼번에 암호화하고 복호화하는 것은 시스템에 과중한 오버헤드를 초래할 수 있다. 본 논문에서는 과중한 오버헤드를 줄이고 사용자의 데이터를 보호하기 위하여 사용자 데이터의 일부만을 암호화하고 복호화 하는 방법을 제안한다.

본 시스템은 키관리 에이전트, 업로드 에이전트, 디스크 매니저, 다운로드 에이전트로 구성된다. 아래의 [그림 3]은 시스템의 구성을 보여준다.



[그림 3] 제안 시스템의 동작 과정

모든 사용자는 사용자 등록시 키관리 에이전트에 자신의 개인키와 쌍을 이루는 공개키를 생성하여 등록한다.

업로드 에이전트에서는 다음과 같은 순서로 동작 한다.

① 저장하려는 사용자의 데이터를 여러 개의 블록으로 분할한다.

② 분할된 블록 중 임의의 한 블록의 해쉬값을 생성한다.

③ 해쉬값이 생성된 블록을 키관리 센터에 등록되어 있는 사용자의 공개키로 암호화한다.

④ 해쉬값과 암호화된 블록을 포함한 데이터 블록들을 디스크 매니저로 전달한다.

디스크 매니저는 전달받은 여러 개의 데이터 블록과 해쉬값을 스트라이핑을 이용하여 저장한다. 스트라이핑은 분할된 블록들을 여러 디스크에 분산 저장하는 방법으로 읽기와 쓰기 트랜잭션이 빈번한 클라우드 저장 방식에 적당하다.

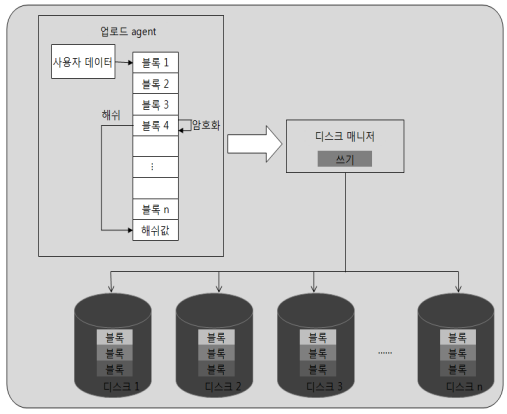
업로드 에이전트와 디스크 매니저의 동작은 다음 그림과 같다.

다운로드 에이전트는 다음과 같이 동작한다.

① 스트라이핑 방식으로 여러 개의 디스크에 저장된 데이터에 대해 사용자의 다운로드 요청이 있으면 다운로드 에이전트는 사용자의 개인키를 사용자에게 입력받는다.

② 스토리지에 저장된 데이터 블록 중 암호화된 데이터 블록을 입력받은 사용자의 개인키로 복호화 한다.

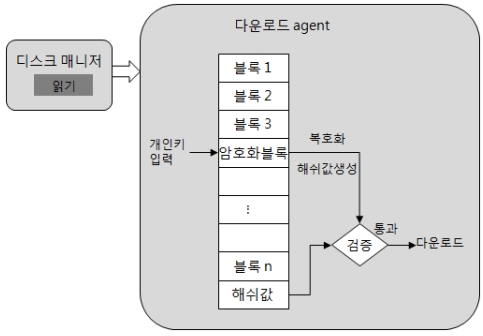
③ 복호화된 데이터의 해쉬값을 생성하고 저장된 해쉬값과 검증한다.



[그림 4] 업로드 에이전트와 디스크매니저

④ 해쉬값 검증이 완료되면 복호화된 데이터 블록을 포함한 모든 데이터 블록들을 순서에 맞게 배열하여 사용자에게 전송한다.

다운로드 에이전트는 아래의 그림과 같이 동작한다.



[그림 5] 다운로드 에이전트의 동작과정

4. 제안 시스템의 안전성 분석

본 장에서는 제안 기법과 기존 어플리케이션 검증 및 관리 기법을 비교 분석하여 평가한다.

클라우드 시스템은 사용자의 데이터를 다양한 방식으로 언제어디서든 접근할 수 있는 편리한 방법이지만 보안성의 측면에서는 사용자가 자신의 데이터가 저장되는 위치에 대해 알 수 없고 복제되는 내역을 알지 못하고 클라우드 서버 관리자가 사용자의 데이터에 임의로 접근하는 것을 막는 것이 불가능하다는 한계들이 존재하므로 사용자의 민감한 개인 데이터들이 관리자들에게 노출되

는 피해를 입을 수 있다.

제안하는 시스템은 사용자 데이터를 블록으로 분할하여 그중 한 블록에 대해서만 공개키 암호방식을 이용하여 암호화하여 저장하므로 사용자 개인의 데이터에 대한 기밀성을 보장할 수 있게 하였다. 또한 클라우드 데이터 서버에 저장된 사용자 데이터에 대한 접근, 복사, 이동, 수정을 막을 수 있고 해쉬값 검증을 통하여 사용자 데이터에 대한 무결성을 제공한다.

제안하는 시스템에 대한 안전성은 2장에서 설명했던 클라우드 시스템의 보안 요구사항 들을 만족시키는 것을 보임으로써 증명한다.

〈표 3〉 안전성 분석표

구분	보안 기능	내용
기밀성	○	공개키 암호화 방식을 이용하여 암호화
무결성	○	데이터 저장시 생성된 해쉬와 사용자가 복호화한 데이터의 해쉬를 검증함으로 무결성 제공
가용성	○	여러 개의 블록으로 분할하여 스트라이핑 방식으로 사용자 데이터 저장
사용자 인증 및 접근 제어	○	공개키 암호방식을 이용한 암호방식을 사용하므로 사용자에 대한 인증과 접근 권한 관리

공개키 암호화 방식을 이용하여 분할된 블록 중 일부를 개인키와 쌍을 이룬 공개키로 암호화하는 방식으로 기밀성 분할된한다.

데이터의 업로드시 분할된 블록 중 임의의 한 블록의 해쉬값을 생성하여 저장하고 다운로드시 사용자가 복호화된 데이터의 해쉬값을 생성하고 저장된 해쉬값과 검증하므로 데이터의 무결성을 제공한다,

또한 공개키와 쌍을 이룬 개인키를 가진 사용자가 아니면 데이터에 접근할 수 없으므로 권한이 없는 사용자에 의한 데이터의 오류 및 변조가 불가능하다.

사용자의 데이터에 대한 저장방식을 여러 개의 블록으로 분할하여 스트라이핑 방식으로 저장하므로 읽기와 쓰기와 같은 트랜잭션이 빈번한 클라우드 저장 방식에 가용성을 높인다.

공개키 암호방식을 이용한 암호방식을 사용하므로 개인키를 가진 사용자만이 데이터에 접근이 가능하므로 사용자에 대한 인증과 접근 권한 관리가 가능하다.

5. 결 론

사용자 데이터를 클라우드 데이터 서버에 저장하는 것은 다양한 단말기와 유무선 네트워크를 사용하여 언제 어디서나 이용 가능하다는 측면에서 사용자에게 굉장히 편리한 방법이지만 보안성의 측면에서는 사용자가 자신의 데이터가 저장되는 위치에 대해 알 수 없고 복제되는 내역을 알지 못하는 등의 한계가 있을 수밖에 없다.

또한 클라우드 데이터 서버 관리자가 사용자의데이터에 임의로 접근하는 것을 막는것이 불가능하다. 때문에 사용자의 민감한 개인 데이터들이 관리자들에게 노출되는 피해를 입을 수 있다.

본 논문에서는 이러한 점들을 극복하기 위하여 사용자 데이터를 블록으로 분할하여 그중 한 블록에 대해서만 공개키 암호방식을 이용하여 암호화하여 저장하므로 사용자 개인의 데이터에 대한 기밀성과 무결성을 보장할 수 있는 시스템을 제안하였다.

본 시스템은 클라우드 데이터 서버에 저장된 사용자 데이터에 대한 접근, 복사, 이동, 수정을 막을수 있고 대용량의 데이터를 한꺼번에 암호화하고 복호화할 경우 나타나는 시스템의 과중한 오버헤드를 줄일 수 있도록 사용자 데이터의 일부만을 암호화하고 복호화 하는 방법을 제안하였다.

블록의 일부만을 암호화하는 방식이므로 복구 시스템에 대한 고려가 필요하며 사용자 데이터 암호화와 복호화에 사용되는 개인키와 공개키의 효율적인 관리 메커니즘이 필요하다.

참 고 문 헌

[1] 민욱기, 김학연, 남궁한 (2009), 클라우드 컴퓨팅 기술 동향, 전자통신동향분석 제24권 제4호

[2] 정순기, 정만현, 조재익, 손태식, 문종섭 (2011), 클라우드 컴퓨팅 가상화 보안을 위한 아키텍처 구성 및 기능 분석 연구, 보안공학연구논문지, 제8권 제5호

[3] 정제호 (2008), 클라우드 컴퓨팅의 현재와 미래 그리고 시장 전략, 한국소프트웨어 진흥원

[4] 김홍성, 김형식 (2012), 사용자 데이터 기밀성을 보장하기 위한 클라우드 스트리지 게이트웨이, 정보보호학회논문지, 제22권, 제1호

[5] NIST (2011),Guidelines on Security and Pravacy in

Public cloud Computing, Draft Special Publication 800-400
[6] Cloud Security Alliance (2010),Top Threat of Cloud Computing V 1.0
[7] Gartner,Assessing the Security Risks of Cloud Computing (2008), http://www.gartner.com/DisplayDocument?id=685308.
[8] 유우영 (2012), 클라우드 컴퓨팅 서비스 제공자의 개인정보관리체계 개선 방안에 대한 연구, 석사학위논문, 고려대학교

이 애 리

- 1997년 2월: 세명대학교 전자계산학과(이학사)
- 1999년 8월: 세명대학교 전산교육과(교육학석사)
- 2007년 2월: 명지대학교 컴퓨터공학과(공학박사)
- 1999년 9월~현재: 세명대학교 컴퓨터학부 강사
- 관심분야: 네트워크 보안, 클라우드 시스템, 정보보호,M2M
- E-Mail:allee@naver.com

조 도 은

- 1997년 2월: 충주대학교 컴퓨터공학과(공학사)
- 2001년 8월: 세명대학교 전산교육학과(교육학석사)
- 2007년 2월: 충북대학교 컴퓨터공학과 (공학박사)
- 2008년 3월~현재: 목원대학교 공학교육혁신센터 조교수
- 관심분야: 정보보호, 유비쿼터스보안, USN, 스마트그리드
- E-Mail: decho@mokwon.ac.kr

이 재 영

- 1996년 2월: 세명대학교 전자계산학과(이학사)
- 1998년 3월: 세명대학교 전산교육학과(교육학석사)
- 2007년 2월: 충북대학교 컴퓨터공학과 (공학박사)
- 2012년 9월~현재: 세명대학교 교양과정부 조교수
- 관심분야 : 정보보호, 클라우드, 네트워크 보안, 스마트그리드
- E-Mail: klitie@semyung.ac.krr