Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1149

클라우드 플랫폼 환경에서의 프라이버시 보호기법 연구 동향 및 전망*

박 태 환,† 이 가 람, 김 호 원‡
부산대학교 전기전자컴퓨터공학과

Survey and Prospective on Privacy Protection Methods on Cloud Platform Environment*

Tae-hwan Park,† Ga-ram Lee, Ho-won Kim‡
Pusan National University Department of Electrical and Computer Engineering

요 약

최근 활발하게 연구 및 개발 중인 사물인터넷 기술에 있어서 아마존의 AWS, IBM의 Bluemix와 같은 클라우드 플랫폼들이 원활한 서비스 제공을 위해 많이 사용되고 있다. 이러한 클라우드 플랫폼 환경의 사용 증가에 따라 여러 보안 위협들이 제기되고 있다. 본 논문에서는 클라우드 환경 상에서의 보안기술 및 개인정보보호 기법에 대한 연구와 관련 제도 및 법률적 연구의 동향을 살펴보며, 이를 바탕으로 기술적, 법률적 측면에서의 향후 클라우드 플랫폼 환경에서의 보안 및 프라이버시 보호 기법 연구에 대한 전망을 제시한다.

ABSTRACT

In these days, cloud environments such as cloud platforms, cloud services like Amazon AWS, IBM Bluemix are used in the Internet of Things for providing efficient services. These cloud platform environments have various security threats according to increasing of use, so the recent research results on cloud security and privacy protection technologies and related regimes and legislations are written in this paper and we suggest prospect of research on cloud platform environment security and privacy preserving.

Keywords: Cloud Platform, Privacy, Security, IoT, Cloud Service

I. 서 론

최근 주위의 모든 사물(디바이스)들이 유·무선 네트워크를 통해 다양하고 수많은 데이터를 송·수신 또는 특정 서버에 저장하고 있다. 또한 이를 활용해 해당 디바이스 사용자들에게 또는 사물 주변 사람들에게 다양한 응용 서비스나 정보를 제공하고 있다. 이러한 서비스 및 기술을 우리는 사물인터넷(IoT:Internet of Things)이라고 부르고, 현재 사물인터넷을 활용한 수많은 서비스와 디바이스에 대해 활발한 연구 및 개발이 진행 중에 있다. 사물인터넷 상에서 발생하는 많은 데이터를 저장하고 이러한 데이터를 분석하여 우리에게 필요한 데이터로 변환 할 필요가 있다. 따라서 데이터의 저장 및 분석을 위해 최근에는 클라우드라 불리는 가상의 서버 환경을 활용하고 있다. 클라우드 서비스는 무형의 형태로 존재하는 하드웨어·소프트웨어 등 컴퓨팅 자원을 필요한 만큼 빌려 쓰고 사용요금을 지급하는 서비스로, 가상

Received(05. 15. 2017), Modified(06. 20. 2017), Accepted(06. 23. 2017)
* 본 논문은 2017년도 영남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임
* 본 연구는 2017년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 20152000000170)
† 주저자, pth5804@pusan.ac.kr
‡ 교신저자, howonkim@pusan.ac.kr(Corresponding author)

화 기술을 통해 컴퓨팅 자원을 통합하여 서비스를 제공하는 것을 의미한다. 그리고 클라우드 플랫폼의 경우, 이러한 클라우드 서비스를 이용하여 애플리케이션을 만들기 위해 필요한 기술 및 도구 집합을 의미한다. 클라우드 서비스는 가상화 기술을 이용한 서비스이기 때문에, 가상화 서비스에 따른 프라이버시 정보 보호에 관한 문제가 발생할 가능성이 아주 높다. 이러한 프라이버시 문제는 클라우드 서비스 및 클라우드 플랫폼의 이용자가 많아지고 있는 현 상황에서 더욱 중요한 문제로 작용하고 있으며 해결 할 필요가 있다. 본 논문에서는 현재 클라우드 환경 상에서 발생할 수 있는 여러 보안 위협 요소에 대해 알아보고, 이 중 프라이버시 보호 기법에 대한 연구 동향 및 전망에 대해 중점적으로 다룰 것이다. 본 논문의 구성은 다음과 같다. 2장에서 클라우드 플랫폼 보안기술과 프라이버시 보호기법에 대한 연구동향에 살펴보며, 3장 본론에서는 클라우드 플랫폼 상 보안 및 프라이버시 보호 문제와 클라우드 플랫폼 상에서의 프라이버시 보호기법 연구 전망에 대해 살펴본다. 마지막 4장에서 본 논문의 결론을 제시한다.

II. 클라우드 환경에서의 보안 연구 동향

본 장에서는 클라우드 플랫폼에 대한 기존의 보안 연구 및 기술과 프라이버시 보호기법 연구 동향에 대해 살펴본다.

2.1 클라우드 플랫폼 보안 연구 동향

클라우드 플랫폼 기술은 클라우드 컴퓨팅 기술의 한 분류이며, 클라우드 플랫폼 기술은 서비스 배치 및 관리 기술, 클라우드 분산 시스템 기술과 클라우드 보안 기술로 구성된다[1]. 클라우드 플랫폼 보안의 요소기술은 기밀성 및 데이터 암호화, 사용자 인증과 접근제어, 데이터의 무결성, 가용성 및 복구, 원격 확인 및 가상 머신 보호, 네트워크 보안 및 웹 보안 등으로 구성된다[1]. 클라우드 컴퓨팅 보안기술로는 안전한 가상화 기술, 저장 데이터 보호 기술, 인증 기술, 관리기술 등이 있다[2]. 가트너에서는 클라우드 컴퓨팅의 보안 위협 평가를 위한 가이드라인을 제시하고 있다[1]. 2011년 10월에는 한국인터넷진흥원(KISA)에서는 “클라우드 서비스 정보보호 안내서”를 발간하였다[3, 4]. 클라우드 플랫폼의 보안에 대해, 개인 사용자 관점에서는 개인정보 노출, 개인에 대한 감시, 개인 데이터에 대한 상업적 목적의 가공 등의 문제가 발생할 수 있으며, 기업의 경우, 서비스 중단, 고객의 정보 훼손/유출 문제가 발생할 수 있다[5]. 클라우드 플랫폼 보안의 대표적인 사례로는 아마존 웹 서비스(Amazon Web Service, AWS)가 있으며, AWS의 경우, 물리적 보안, 백업, EC2 보안, S3 보안, DB 보안 등의 기술을 적용하고 있는 것으로 확인되었다[3, 5]. IBM의 Bluemix의 경우, Bluemix 인프라(소프트 계층)기반의 기능적, 수행적, 물리적 보안을 제공한다[2]. 특히 물리적 보안의 경우, Gemalto사의 SafeNet HSM(Hardware Security Module)을 기반으로 하여 암호화 키 및 중요 데이터에 대한 보호기능을 제공하고 있다[4]. Bluemix 플랫폼 보안의 경우, ACL(Access Control List)를 기반으로 한 접근제어, 사용자 인증 및 인가 기능과 DoS(Denial of Service) 및 시스템 공격에 대한 보호기능을 제공하고 있다[2]. 구글의 클라우드 플랫폼인 구글 앱 엔진의 경우, 구글 클라우드 키 관리 서비스를 통해, 클라우드 플랫폼 상의 데이터 암호화 및 암호화 키 관리를 통한 보안성을 제공하고 있다[6]. 마이크로소프트의 경우, 애저 키 벨류(Azure Key Value)와 같은 클라우드 키 암호화 도구를 통해, 클라우드 플랫폼인 Azure 상의 데이터 암호화를 제공하고 있으며, 역할 기반 엑세스 제어 기능 또한 제공하고 있다[7]. 국내의 경우, 안철수 연구소에서는 클라우드 컴퓨팅 활용 보안 서비스 전략과 위협 대응체계를 발행하였다[8, 9].

2.2 프라이버시 보호기법 연구 동향

기존에 수행되었던 프라이버시 보호기법 연구의 경우, 법적, 제도적 측면에서의 연구결과와 기술적 측면에서의 연구 결과 두 가지의 경우로 나누어질 수 있다.

먼저, 클라우드 서비스와 개인 정보 보호의 문제점에 대해 법적, 제도적 측면에서 분석한 연구 결과 및 관련 사례로서, 개인정보 보호에 관한 국내 법제 분석 결과를 제시하고 있다[10, 11]. 그리고 클라우드 컴퓨팅 환경 상에서의 보안 관리를 위한 가이드라인 연구 및 가이드라인을 제시한 연구[12]가 있으며, 클라우드 컴퓨팅 환경에서의 개인정보보호 조치 방안에 대한 연구 결과가 있다[13]. 클라우드 서비스 상에서의 프라이버시 침해 요인을 고객 정보 및 서비스 정보 수집 단계부터 서비스/시스템 관리 단계, 서비스 무선 통신 및 시스템 관점에서의 프라이버시 침해 요인을

분석하고 관리적, 기술적 침해 대응 방안을 제시한 연구 결과[14]가 있다. 클라우드 컴퓨팅과 관련한 국제 표준에 따른 보안 표준화 동향에 대한 연구가 있다[15]. 그리고 정보 보호 관리 체계(ISMS)에 대한 국제표준인 ISO 27002의 내용과 KISA-PIMS를 바탕으로 클라우드 환경에서의 개인정보보호 위협 및 위협에 대응하기 위한 다양한 보안요구사항들을 도출한 결과가 있다[21]. 클라우드 환경 상에서의 보안 인증 스키마와 관련한 미국 연방 정보 보안 관리법(FISMA)와 국제 표준인 ISO 27001 그리고 미국 연방정부의 클라우드 제품 및 서비스 등에 대한 보안성 평가, 인증, 모니터링 시스템인 FedRAMP, 클라우드 보안 연합체에서 발표한 CSA-CCM 등을 분석한 연구가 있다. 또한 분석된 결과를 바탕으로 다양한 표준 및 제도적 측면에서 클라우드 환경에서의 보안 인증에 대한 해결 과제를 제시하고 있다[23]. 이러한 법적, 제도적 측면에서의 연구는 클라우드 서비스와 관련된 국내법제 분석 연구, 보안 관리를 위한 가이드라인 및 조치 방안에 대한 연구가 있으며, 정보보호 관련 국제표준들을 바탕으로 클라우드 환경에서의 보안성을 강구하기 위한 연구가 진행되었다.

기술적인 측면에 있어서는 모바일 RFID 네트워크 환경 상에서의 프라이버시 문제점 분석 및 프라이버시 보호기법을 제시한 연구 결과[16]가 있으며, RFID 시스템 상에서의 프라이버시 보호기법 제안 논문[19]과 저가형 RFID 환경에서의 효율적인 프라이버시 보호 프로토콜을 제안 논문이 있다[20]. 또 다른 프라이버시 보호기법 연구는 소셜 네트워크 환경에 대한 연구가 있으며, 소셜 네트워크 상에서의 데이터 배포 시 프라이버시 보호를 위한 l-차수 다양성 모델 기반 프라이버시 보호 기법 제안 논문[17]이 있으며, 준 동형 공개키 암호 시스템을 적용하여 암호화된 데이터에 대한 검색 기능 및 접근 제어 기능을 통한 효율적인 프라이버시 보호 데이터 공유 기법에 대한 연구 결과가 있으며[18], 정수 기반 동형 암호 기법을 적용하여 데이터 기밀성과 검색 기능을 동시에 제공하는 연구 또한 있다[27]. 사용자 데이터 블록화 및 공개키 암호화 방식 기반의 데이터 기밀성 및 무결성 제공을 통한 사용자 데이터 보호 방안을 제시한 연구가 있다[22]. 클라우드 환경에서 이미지 프라이버시 보호를 위해, 경량화된 이미지 암호화 기법을 제안하고 있으며[24], 클라우드 환경 상에서 스트리밍 미디어 검색이 가능한 이미지 암호 시스템 또한 제안되었다[25]. 클라우드 스토리지 상에서의 기존 인증 기반 무결성 검증 기법의 취약점을 보완하는 새로운 무결성 검증 기법 제시를 통한 안전성을 제공하는 연구가 있다[26]. 모바일 클라우드 컴퓨팅 환경에서 사용자의 생체 정보(음성)과 개인 신원 및 권한 인증 기법을 결합한 2-factor 인증 방식을 제안한 연구 결과 또한 있다[28]. 프라이버시 보호 방안에 대한 기술적 연구는 데이터 암호화, 접근제어, 데이터 무결성, 인증/인가 기술에 대한 연구가 진행되었다.

III. 본 론

본 장에서는 클라우드 환경 중 클라우드 플랫폼 상의 보안 문제 및 프라이버시 보호 문제를 살펴보고 클라우드 플랫폼 상에서의 프라이버시 보호기법 연구 전망에 대해 살펴본다.

3.1 클라우드 플랫폼 보안 문제

클라우드 컴퓨팅 환경에서 확인해야 되는 보안 위험 혹은 문제의 경우, 특권 사용자 접근 관리, 규정 준수성, 데이터의 입지, 데이터의 격리, 복구 계획, 조사 가능성, 장기적 경쟁력이 있다[12]. 클라우드 컴퓨팅 보안 취약점에 대해 NIST, 가트너 등에서 발간한 클라우드 컴퓨팅의 대표적인 보안 취약점은 가상화 취약점, 정보위탁에 따른 정보 유출 위협, 자원 공유 및 집중화에 따른 서비스 장애, 단말 다양성에 따른 정보 유출, 분산 처리에 따른 보안 적용의 어려움, 법규 및 규제의 문제 등이 있다[8].

3.2 클라우드 플랫폼 프라이버시 보호 문제

클라우드 플랫폼 서비스 상에서의 개인정보보호 고려사항은 개인정보의 물리적 저장 위치, 개인정보 보관 위치에 따른 해외 이전 이슈, 개인정보의 보존 및 파기와 같은 문제[13]에 대해 고려해야한다. 그리고 앞선 3.1.에서의 클라우드 플랫폼 상 보안 문제 중 특권 사용자 접근 관리, 데이터의 입지와 격리, 정보 위탁에 따른 정보 유출 위협, 단말 다양성에 따른 정보 유출 등이 클라우드 플랫폼 상에서의 프라이버시 보호 문제와 연관되어있다. 즉, 사용자의 데이터에 대한 보관 및 처리 과정에서 프라이버시 보호와 관련된 보안문제가 발생할 수 있다.

이러한 보안 문제점을 해결하기 위해 국내의 경우, 개인정보보호법[29]과 정보통신망법[30]을 바탕으로

프라이버시 보호 문제에 대한 법률적 장치를 마련하였다. 개인정보보호법의 경우, 2014년 주민등록번호 수집금지, 주민등록번호 외 기타 개인 식별 번호(여권번호, 운전면허증 번호 등)에 대한 DB 암호화 및 내부망 개인정보 암호화를 필수적으로 지켜야하는 것으로 개정 되었다.

정보통신망법의 경우, 제28조 개인정보의 보호조치를 통해, 개인정보에 대한 접근 통제 장치 설치 및 운영, 접속기록에 대한 위/변조 방지, 데이터 암호화 등 개인정보 보호조치에 대한 내용을 명시하고 있으며, 정보통신망법 시행령 4장 개인정보의 보호 제9조의 2항에서 중요정보에 대한 분류 및 접근권한의 범위를 지정하고 있으며, 이에 대한 조치를 법적으로 지정하고 있다. 이러한 국내법들과 더불어 국가 공공기관 및 금융기관의 경우, 전자정부법 제56조, 동법 시행령 69조와 전자금융감독규정 제15조에 의거하여 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 적용해야하며, 국가정보원에서 규정한 검증필 암호모듈의 탑재가 필요한 상황이다. 이러한 관련 법규와 더불어 암호모듈검증제도 및 국정원 보안적합성 평가를 거친 제품이 납품되어야하는 상황이다. 이러한 상황에서 관련법을 준수한 보안 제품군들은 데이터베이스 환경에 한정되어있는 상황이며, 대표적인 사례[31]는 오라클 라벨 시큐리티(Oracle Label Security) 솔루션으로 DB 접근제어 및 데이터 암호화를 지원하고 있으며, 파수닷컴의 경우, DB쿼리 암호화를 지원하는 '솔리드베이스(Solidbase)'와 DB 접근제어 솔루션 '페이스(Face)'가 있는 상황이다. 즉, 클라우드 플랫폼에 대한 개인정보보호법 및 정보통신망법에서 요구하는 데이터 암호화, 접근제어, 인증/인가 등의 기술 적용이 필요한 상황이며, 이를 통해 암호모듈검증제도 및 국정원 보안적합성 평가를 거친 클라우드 플랫폼 제품 개발이 필요한 상황이다. 이를 위한 각각의 보안 기술(데이터 암호화, 접근제어, 인증/인가 등)에 대한 연구는 많이 되어있지만, 클라우드 플랫폼 환경으로의 적용 및 적용 시 발생할 수 있는 이슈들에 대한 연구가 필요할 것으로 보인다.

3.3 클라우드 플랫폼 상에서의 프라이버시 보호기법 연구 전망

앞선 2장에서 클라우드 플랫폼 보안 연구 동향 및 프라이버시 보호기법 연구동향에 대해 법적, 제도적 연구 측면과 기술 연구 측면으로 나누어 살펴보았다. 이를 통해, 클라우드 플랫폼 제품의 경우, 아마존의 AWS, IBM Bluemix, 구글 앱 엔진 및 마이크로소프트 애저와 같은 기업의 제품에서 보안성을 제공하는 것으로 확인되었다. 클라우드 플랫폼 환경에서의 보안을 위한 요소기술 및 보안을 위한 법적, 제도적인 방안이 마련되어있으며, 관련 국제 표준을 기반으로 한 클라우드 환경 보안성 강화 연구가 이루어지고 있는 것으로 확인되었다. 기술 연구 측면에서는 데이터 암호화, 접근제어, 데이터 무결성 및 인증/인가 기술에 대한 연구가 활발히 진행되고 있는 것으로 확인되었으며, 3.1과 3.2절에서 살펴본 클라우드 플랫폼 보안 및 프라이버시 보호 문제의 경우, 국내 개인정보보호법과 정보통신망법에서의 요구사항인 개인정보에 대한 암호화, 접근제어, 인증/인가, 위/변조 방지 등과 국가정보원에서 규정한 검증필 암호모듈 탑재와 보안적합성 평가 관점에서의 연구가 미흡한 것으로 파악되었다. 대표적인 예로 오라클 라벨 시큐리티와 파수닷컴의 솔리드베이스, 페이스와 같은 솔루션 제품은 데이터베이스 환경에 맞춰진 제품인 상황이며, 앞서 살펴본 클라우드 플랫폼 제품의 경우, 개인정보보호법 및 정보통신망법에서의 보안 요구사항을 만족하지만, 검증필 암호모듈 미탑재, 국가정보원 보안적합성 검증 및 CC인증 제품이 아니라는 단점을 가지고 있어 정부 및 공공기관에서 활용하기에 어려움이 있다. 이러한 문제점을 해결하기 위해서는 기술 연구 측면에서의 검증필 암호모듈 및 무결성 검증기법에 대한 클라우드 플랫폼 환경 적용 및 최적화 연구가 필요하며, 데이터 무결성 기법 또한 클라우드 플랫폼 환경에 클라우드 플랫폼 환경에 적합한 접근제어, 인증/인가 기술 연구가 필요할 것으로 생각된다. 법적, 제도적 측면에서의 연구에서는 현재 국내 개인정보보호법, 정보통신망법 등 관련 법안의 클라우드 플랫폼 환경 및 관련 분야로의 적용을 위한 방안과 관련 법, 제도 개정 등을 위한 연구가 필요할 것으로 보인다. 클라우드 플랫폼 환경에서의 보안을 위한 관련 국내 표준화를 통해, 클라우드 플랫폼 보안에 대한 기술 및 법적, 제도적 장치 마련이 필요하다고 생각된다.

IV. 결 론

본 논문에서는 기술 연구 측면과 법적, 제도적 연구 측면에서 클라우드 플랫폼 환경에서의 보안 및 프

라이버시 보호를 위한 연구 동향을 살펴보았다. 아마존, IBM, 구글, 마이크로소프트와 같은 글로벌 기업의 클라우드 플랫폼 제품에서는 보안성 제공을 위한 암호화, 접근제어 등의 다양한 보안기술을 적용하고 있으며, 기술 연구의 경우, 보안성과 프라이버시 보호를 위한 암호화, 접근제어, 무결성 기법 등이 활발히 연구되고 있다. 법적, 제도적 측면에서는 다양한 보안 이슈에 대해 국내의 개인정보보호법과 정보통신망법을 기준으로 관련 보안 요구사항과 관련 제품 현황을 중심으로 살펴보았다. 이를 통해, 기술적 측면에서의 연구는 보안 및 프라이버시 보호를 위한 연구가 활발히 이루어지며, 법적, 제도적 측면에서의 연구는 관련 법률 및 표준화 등의 제도를 기반으로 클라우드 플랫폼 환경에서의 보안을 위한 연구가 진행되고 있는 것으로 확인되었다. 하지만, 클라우드 플랫폼 보안 제품의 경우, 국내의 개인정보보호법과 정보통신망법에서의 요구사항을 만족할 수 있는 제품이 거의 없는 것으로 확인되었으며, 대부분의 제품이 데이터베이스 환경에 집중되어있는 것을 확인할 수가 있었다. 이러한 현황 분석을 통해 향후 국내법을 준수 할 수 있는 클라우드 플랫폼 보안성 확보를 위해, 관련 보안기술의 적용 연구와 클라우드 플랫폼 환경의 변화에 따른 법적, 제도적 측면에서의 개선 연구 및 관련 국내 표준화 연구가 필요할 것으로 생각된다.

References

〔1〕 Cheol-soo Lim, "Cloud computing security technologies," Review of KIISC, 19(3), pp. 14-17, Jun, 2009.

〔2〕 IBM, "IBM Bluemix security," https://console.ng.bluemix.net/docs/security/index.html#security (accessed MAY 13 2017)

〔3〕 Jae-gyu Choi and Bong-nam Noh, "Security technology research in cloud computing environment," Journal of Security Engineering 8(3), pp. 371-384, Jun, 2011.

〔4〕 IBM, "IBM Bluemix Hardward Security Module(HSM)," https://www.ibm.com/cloud-computing/bluemix/ko/node/2361 (accessed MAY 13 2017)

〔5〕 Sung-kyung Eun, "Trend of cloud computing security Technologies," Review of KIISC, 20(2), pp. 27-31, Apr, 2010.

〔6〕 Geun-mo Park, "Google Open the Key Management System(KMS) on Cloud," Korea IT & Industry News, (2017.01.12.), http://www.kinews.net/ news/article-View.html?idxno=102595 (accessed 13 MAY 2017)

〔7〕 Microsoft Azure (2017.04.27.), "Azure Security Document," https://docs.mic rosoft.com/ko-kr/azure/security/azure-security (accessed MAY 13 2017)

〔8〕 Tae-sik Son and Jong-bin Ko, "Trend of IoT (Internet of Things) security on cloud computing," Review of KIISC 22(1), pp. 20-30, Feb, 2012.

〔9〕 Sung-jae Jeong and Yu-mi Bae, "Trend analysis of Threats and Technologies for Cloud Security," Journal of Security Engineering, 10(2), pp. 199-212, Apr, 2013.

〔10〕 Yeun-Dek Chung, "The legal study of protection of personal infomation in cloud computing service," Review of Korea Association For Informedia Law, 15(3), pp. 31-54, Feb, 2012.

〔11〕 Kee-chang Kim, "Cloud service and protection of personal data," Policy research report for improvement of personal information protection law(Privacy Policy Research Forum), pp. 72-83, Feb, 2013.

〔12〕 Hak-bum Kim, Eun-jung Jeon and Sung-jun Kim, "Study on security management in cloud computing environment," Management Consulting Review, 2(1), pp. 127-144, Feb, 2011.

〔13〕 Woo-yong Yu and Jong-in Lim, "A study on the privacy security management under the cloud computing service provide," Journal of the Korea Institute of Information Security and Cryptology, 22(2), pp. 337-346, Apr, 2012.

〔14〕 Jeong-hoon Jeon, "A study on the privacy threats factors of cloud services," Convergence Security Journal,

15(5), pp. 87-95, Sep, 2015.
〔15〕 Heung-yeol Yeom and Mi-yeon Yoon, "Trend of international standard on cloud computing security," Review of KIISC, 23(3), pp. 14-18, Jun, 2013.
〔16〕 Il-jung Kim, Eun-young Choi and Dong-hoon Lee, "A RFID privacy protect scheme based on mobile," Journal of the Korea Institute of Information Security and Cryptology, 17(1), pp. 89-96, Feb, 2007.
〔17〕 Min-kyong Seong and Yeon-don Jung, "A model for privacy preserving publication of social network data," Journal of KIISE : Database, 37(4), pp. 209-219, Aug, 2010.
〔18〕 Doo-hyun Jeon, Ji-young Chun and Ik-rae Jeong, "An efficient privacy-preserving data sharing scheme in social network," Journal of the Korea Institute of Information Security and Cryptology, 22(3), pp. 447-461, Jun, 2012.
〔19〕 Seung-koo Lee, Sang-soo Yeo, Jung-sik Cho and Sung-kwon Kim, "Secure and efficient privacy protection scheme in RFID system," Proceeding of KIISE: Korea Computer Congress, A, pp. 196-198, Jul, 2005.
〔20〕 Sang-jin Lee, Jin Kim and Kwang-jo Kim, "An efficient privacy protection scheme for low-cost RFID," Proceeding of KIISC Summer Information Security Conference, pp. 569-573, Jun, 2005.
〔21〕 Dae-ha Park and Tae-seok Baek, "Trend and assignment of cloud computing privacy protection research," Review of KIISC, 21(5), pp. 37-44, Aug, 2011.
〔22〕 Ae-ri Lee, Do-eun Cho and Jae-young Lee, "A study on the protection of user data in the cloud system," Journal of digital convergence, 10(11), pp. 389-394, Dec, 2012.
〔23〕 Jong-hwei Shin, "Cloud security authentication and assignments," Review of KIISC, 22(6), pp. 28-33, Oct, 2012.
〔24〕 Jang-young Chung and Young-sik Hong method, "Distributed image encryption schemes for privacy-preserving of ultra high resolution images in cloud environments," Journal of Korean Institute of Information Scientists and Engineers: Reality and Letter of Computing, 20(4), pp. 262-266, Apr, 2014.
〔25〕 Byung-rae Cha, Dae-kyu Kim, Nam-ho Kim, Se-ill Choi and Jong-won Kim, "Design of searchable image encryption system of streaming media based on cloud computing," Journal of Korea Institute of Electronic Communication Sciences, 7(4), pp. 811-819, 2012.
〔26〕 Mok-ryeon Baek, Dong-min Kim and Ik-rae Jeong, "Privacy-preserving self-certified public auditing for secure cloud storage," Journal of KIISE, 43(4), pp. 497-508, Apr, 2016.
〔27〕 Hyun-sung Kim and Sung-woon Lee, "Homomorphic encryption scheme and applications for cloud computing security," Journal of Security Engineering, 10(2), pp. 213-224, Apr, 2013.
〔28〕 Hyun-mi Jung, Jae-in Sin and Gang-soo Lee, "Design of user authentication method in mobile cloud computing," Proceeding of Korea Institute of Multimedia, 2010(2), pp. 516-519, 2010.
〔29〕 National Law Information Center, "Personal information protection act," http://www.law.go.kr/eng/engLsSc.do?menuId=2&query=PERSONAL%20INFORMATION%20PROTECTION%20ACT#liBgcolor15, (accessed 19 JUNE 2017)
〔30〕 National Law Information Center, "Act on promotion of information and communications network urilization and information protection, etc," http://www.law.go.kr/eng/engLsSc.do?menuId=2&query=ACT%20ON%20PROMOTION%20OF%20INFORMATION%20AND%20COMMUNIC

ATIONS%20NETWORK%20UTILIZATION%20AND %20INFORMATION%20PROTECTION%2C%20ETC.#liBgcolor0, (accessed 19 JUNE 2017)
[31] Tae-hyung Kim, "'Attention!' db access control solution for protecting personal information leakage", Boannews, 2016.05.17., http://www.boannews.com/media/view.asp?idx=50623, (accessed 19 JUNE 2017)

〈저자소개〉

박 태 환 (Tae-hwan Park) 학생회원
2013년 2월: 부산대학교 정보컴퓨터공학부 학사 졸업
2013년 3월~현재: 부산대학교 전기전자컴퓨터공학과 석, 박사 통합과정
〈관심분야〉 암호화 구현, IoT 디바이스 보안, Post-Quantum Cryptography

이 가 람 (Ga-ram Lee) 학생회원
2016년 2월: 부산대학교 정보컴퓨터공학부 학사 졸업
2016년 3월~현재: 부산대학교 전기전자컴퓨터공학과 석사과정
〈관심분야〉 SW 암호 최적화 구현, IoT 보안, 역공학, 임베디드 보안, 머신러닝

김 호 원 (Ho-won Kim) 종신회원
1993년 2월: 경북대학교 전자공학과 학사 졸업
1995년 2월: 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월: 포항공과대학교 전자전기공학과 박사 졸업
2008년 2월: 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월~현재: 부산대학교 전기컴퓨터공학부 부교수
〈관심분야〉 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안, IoT