정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

클라우드 컴퓨팅 보안 기술 동향

구 동 영*

요 약

IaaS에서부터 SaaS에 이르기까지 디지털 자산을 구축, 배포 및 사용하는 방식이 바뀌면서, 클라우드 컴퓨팅 환경에서의 보안 위협 환경 또한 진화하고 있다. 본 논문에서는 클라우드 컴퓨팅과 관련된 다양한 응용 및 발생 가능한 보안 위협 및 취약점에 초점을 두어 최근 클라우드 컴퓨팅 보안 동향을 살펴본다. 멀티 테넌시와 관련된 고전적 문제에서부터 클라이언트 측 암호화를 통해 손상된 플랫폼의 위험을 완화하려는 노력, 보안 문제에 대한 중앙 집중화의 영향 및 개선 동향에 대해 검토한다.

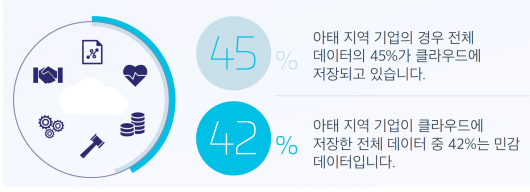
Ⅰ. 서 론

미국표준기술연구소 (NIST)에 따르면, 클라우드 컴퓨팅 (cloud computing)은 구성 가능한 컴퓨팅 자원의 공유 집합에 대하여 어디서나 편리하게 사용자의 요구에 맞추어 네트워크를 통한 접근 및 사용을 가능하게 하는 모델이다[1]. 즉, 저장공간, 연산, 네트워크 등 가상의 컴퓨팅 자원을 인터넷에 연결된 사용자에게 대여하여 사용량에 따른 비용을 부과하는 서비스로 시스템 구입 및 설치, 확장을 위한 노력을 줄이고 물리적 공간을 차지하지 않으면서 신속한 자원 확보 및 서비스 제공이 가능하게 함으로써 유지·관리 비용을 절감할 수 있다는 측면에서 개인을 비롯한 기업에서 활용도가 높아지고 있다.

클라우드 컴퓨팅의 다양한 이점에도 불구하고, 물리적 위치 및 시스템의 내부 구조를 구체적으로 알지 못하는 사용자가 클라우드 서비스 관리자에게 데이터의 관리 및 제어 권한을 전적으로 위임하면서 서비스 제공자 및 사용자 모두에게 다양한 보안 이슈가 발생하고 있다. 2020 탈레스 데이터 위협 보고서에 따르면, [그림 1]에서와 같이 아시아·태평양 지역 기업의 45%가 클라우드에 기업의 전체 데이터를 저장하고, 27%는 2019년 데이터 침해를 경험하였으며 47%는 과거 데이터 침해를 경험한 적이 있다고 응답하였다 [2]. 이처럼 클라우드 컴퓨팅의 도입과 함께 발생하는 새로운 보안 위협에 대한 관심과 대응 방안에 대한 연구는 그 중요성이 더해진다고 볼 수 있다.

클라우드 컴퓨팅 환경에서의 보안 취약점이 꾸준히 발견됨에 따라 이를 해결하기 위한 연구 또한 활발히 진행되고 있는데, 본 논문에서는 클라우드 서비스를 이용하는 다양한 환경과 발생 가능한 보안 문제점을 해결하기 위한 최근 연구 동향을 살펴본다.

2절에서 클라우드 컴퓨팅의 개념을 모델에 따라 정리한 후 클라우드 시스템에서 관심이 집중되고 있는 보안 이슈를 확인한다. 3절에서는 최근 클라우드 사용 환경에서의 보안 문제 해결을 위한 최근 연구 동향을 요약하며, 4절에서 향후 클라우드 컴퓨팅 환경에서 고려해야 할 사항 및 논의로 논문을 마무리한다.



〔그림 1〕 아시아태평양 지역의 클라우드 사용 현황

Ⅱ. 클라우드 컴퓨팅 개요

클라우드 컴퓨팅은 사용 대상 및 서비스 제공 범위에 따라 여러 유형으로 구분될 수 있다.

이 성과는 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2017R1C1B5077026).
* 한성대학교 기계전자공학부 정보시스템 트랙 (조교수, dykoo@hansung.ac.kr)

2.1. 서비스 모델

클라우드 컴퓨팅은 사용자에게 제공하는 컴퓨팅 자원의 범위에 따라 크게 Iaas, PaaS, SaaS의 3가지 서비스 모델로 구분할 수 있다.

IaaS (Infrastructure as a Service)는 운영체제 및 응용 프로그램을 포함하여 프로세싱, 저장장치, 네트워크를 포함한 핵심적인 컴퓨팅 자원에 대한 제어권을 사용자에게 제공하는 서비스이다. 주로 논리적으로 온전한 기능을 수행하는 하나의 컴퓨팅 환경으로, 하나의 물리적 장치에 다수의 가상 머신 (virtual machine, VM) 및 컨테이너를 포함하는 형태로 구성되며 나머지 부분으로부터 격리된 환경이 제공된다.

PaaS (Platform as a Service)는 서비스 제공자로부터 지원되는 프로그래밍 언어, 라이브러리, 기타 서비스, 및 툴을 이용하여 사용자가 제작하거나 획득한 응용 프로그램을 클라우드 인프라에 배포할 수 있는 권한을 제공하는 서비스이다. 사용자는 네트워크, 서버, 운영체제, 저장장치를 포함한 클라우드 인프라에 대한 관리 및 제어권은 없으나 응용 프로그램 운영을 위한 환경 설정과 해당 응용 프로그램에 대한 제어권을 가진다.

SaaS (Software as a Service)는 다양한 사용자 장치로부터 네트워크를 통하여 응용 프로그램을 사용할 수 있는 환경을 제공하는 서비스로, 사용자는 특정 응용의 설정 사항을 포함하여 응용 프로그램이 구동되는 클라우드 인프라에 대한 관리 및 제어가 불가능하다.

2.2. 배포 모델

클라우드 컴퓨팅은 사용 대상 및 배포 형태에 따라 사설/커뮤니티/공용/하이브리드 클라우드로 구분될 수 있다.

사설 클라우드 (private cloud)는 특정 기관에 의하여 배타적으로 운영되는 형태로 컴퓨팅 자원의 제어권을 운영 기관이 가지고 있어, 다른 배포 모델에 비하여 상대적으로 보안 측면에서 강점이 있으며 접근 권한을 부여받은 사용자들만 서비스를 이용할 수 있다.

커뮤니티 클라우드 (community cloud)는 공동의 목적 (임무, 보안 요구사항, 정책, 규정 등)을 공유하는 특정 기관들에 의하여 운영되며, 해당 기관의 구성원들에게만 접근이 허용되는 형태이다.

공용 클라우드 (public cloud)는 공공 대중의 사용을 위하여 개방된 형태로, 인터넷에 접속 가능한 모든 사용자를 대상으로 한다. 서비스 내부에 저장된 데이터나 기능, 컴퓨팅 자원은 각 서비스에서 사용자에 따라 별도의 권한 관리가 이루어지며 서비스 사용자 간에 간섭이 존재하지 않도록 구성된다.

하이브리드 클라우드 (hybrid cloud)는 사설, 커뮤니티, 공용 클라우드의 조합으로 구성된 형태로, 데이터 보안이 중요하거나 컴퓨팅 자원에 대한 제어가 필요한 서비스에서는 사설 클라우드 및 커뮤니티 클라우드를 이용하고 그렇지 않은 환경에서는 공용 클라우드를 이용한다.

2.3. 클라우드 보안 위협

클라우드 서비스를 이용하는 사용자 관점에서는 연산, 처리, 가공 및 저장되며 공격자가 탈취, 변조, 파괴하고자 하는 주요 대상이 데이터이므로 데이터의 기밀성 및 무결성에 대한 보장을 주요 보안 목표로 하고 있으며, 클라우드 서비스 제공자는 원활한 서비스 제공을 위한 가용성 확보를 주목적으로 하고 있다.

클라우드 서비스 취약점은 시스템 구조, 응용 API (application programming interface), 네트워크 채널 등에 존재하는데, 평판 관리를 통한 사용자 유치를 위하여 사용자 및 데이터의 프라이버시 보장을 사용자에게 강조하기 위하여 가상화 보안 등 다양한 보안 매커니즘을 적용하고 있다. 본 논문에서는 서비스 제공자 관점에서 클라우드 시스템의 구조적 결함 및 멀티 테넌시 환경에서 보안 이슈를 살펴보고, 사용자 관점에서 데이터의 프라이버시 보존 및 머신러닝을 활용한 데이터 활용, 암호화 기법의 적용을 대상으로 최근 연구 동향을 살펴본다.

Ⅲ. 클라우드 보안 연구 동향

3.1. 구조적 결함

클라우드에서의 소프트웨어는 주로 지속적 배포 및 DevOps 등을 통한 개발 속도 향상과 신속한 처리가 가능한 민첩 방법론 (agile methodologies)을 적용하고 있다. 개발 속도의 증가에 따라 클라우드 서비스 운영에 지장을 초래하는 보안 버그 및 구조적 결함을 방지하기

위한 소프트웨어 보안에 대한 관심을 소홀해지는 경향이 있다. 클라우드 아키텍처 위험 분석은 대표적인 소프트웨어 보안 활동의 하나로 알려져 있으나 일부 민첩 방법론을 채택한 개발 프로젝트에는 구조 설계자가 없거나 고유한 구조적 활동이 없다. Jaatun은 구조 분석을 수행하는 MS SDL (security development lifecycle), Synopsys Touchpoints 등 민첩 개발 프로젝트에서 구조적 위험 분석을 수행할 때 고려할 사항을 분석하며, 개발 및 설계 단계에서의 구조적 결함 분석 및 위협 모델의 명확화가 필수요소임을 강조하였다 [3].

3.2. 멀티 테넌시 (multi-tenancy) 환경

공개 클라우드는 근본적으로 멀티 테넌시 (multi-tenancy) 환경으로, 공격자를 포함한 다른 사용자에 의해 배포된 응용이 동일한 물리적 장치에 상주하면서 다양한 하드웨어 자원을 공유하게 된다. 최근 새로운 하이퍼바이저 (hypervisor), Docker와 같은 컨테이너화된 프레임워크, Kubernetes와 같은 시스템을 사용하여 관리 및 조직되는 클러스터의 도입으로 클라우드 서비스 제공자는 응용이 하드웨어에서 공유된 상태로 동작하지 않는다고 홍보하며 멀티 테넌시 환경에서의 공격을 중요하게 여기지 않고 있다. Shringarputale 등은 상업적으로 활용되는 다양한 시스템에서 실행되는 컨테이너에 존재하는 취약점을 분석하여, AWS 및 MS Azure를 포함한 상용 클라우드 환경에서 실제 워크로드를 사용하여 90%의 성공 확률로 응용의 공유 상태를 탐지하는 방법을 제시하였으며, 사용자들은 클라우드 서비스 제공자가 제공하는 공유 공격 (co-residency attack)의 내성에 의존하지 않는 안전한 컴퓨팅 환경을 구축할 필요가 있음을 강조하고 있다 [4].

Qin 등은 클라우드 시스템의 응용 공유 환경에서 공격을 탐지하기 위하여 실시간으로 메모리 접근 흔적을 분석하는 이상 탐지기인 MARTINI를 제시하며 여러 유형의 부채널 공격을 포함한 비인가 프로그램의 실행과 밀접하게 관련되어 있음을 보였다 [5]. MARTINI는 실시간으로 읽고 쓰는 메인 메모리의 주소 관점에서 정상적인 프로그램 동작을 모델링하는 유한 오토마타 (finite automata)로 구성되는데, 정상 프로그램의 행동 학습으로부터 소프트웨어 수준에서 탐지하기 어려운 저수준의 비정상 동작 및 공격을 신속히 탐지할 수 있다.

3.3. 머신러닝을 통한 데이터 추론과 프라이버시

데이터 소유자는 사용자의 개인정보보호를 위해 많은 노력을 기울이면서도 우수한 예측률을 가진 머신러닝 모델 생성을 도모하고 있다.

Zhao 등은 차등 개인정보 (differential privacy, DP)의 다양한 구현을 평가하여 분류 성능과 함께 실제 프라이버시 공격 내성을 측정하였다[6]. 저자들은 프라이버시 보존과 데이터 활용 사이에서 바람직한 절충안을 제공하기 위한 구현을 파악하는 과정에서, 더 많은 부류가 존재하는 데이터셋에서 프라이버시 취약점이 증가할 것이라는 직관과 상반되는 추론인 주어진 데이터셋의 부류 (class) 수가 개인정보보호 및 활용성의 절충에 영향을 미치지 않는다는 사실을 발견하였다.

최근에는 제한된 변수 가공만으로도 높은 분류 및 탐지 정확도를 보이는 심층 신경망 (deep neural network, DNN)이 중요한 지적 재산으로 여겨지고 있으며, 이를 활용한 딥러닝 (deep learning, DL) 기술이 침입 탐지 시스템에 적용되는 비중 또한 증가하고 있다. 하지만 딥러닝을 기반으로 하는 탐지 시스템은 공격자가 악의적 트래픽에 미묘한 변화를 추가함으로써 효율적인 탐지를 우회하는 적대적 예제 (adversarial example)에 의한 공격에 취약한 것으로 알려져 있다. Zhang 등은 네트워크 침입 탐지 시스템 (network intrusion detection system, NIDS)을 우회하기 위하여 최신 적대적 공격을 수행하여 35.7%의 공격 성공률을 확인하였다. 그들은 여러 분류기의 결과를 투표를 통하여 적대적 예제로 인한 오분류 확률을 낮추는 모델 투표 앙상블 (model voting ensemble), 적대적 예제를 학습 데이터에 추가하여 재학습하는 강화학습으로 적대적 학습 앙상블 (ensembling adversarial training), 블랙박스 공격 환경에서 질의 과정을 탐지하는 질의 탐지 (query detection)라는 세 가지 새로운 대응 메커니즘을 통합하여 NIDS의 탐지율을 100%에 가까이 높여 적대적 공격에 대한 내성을 증가시키기 위한 연구를 수행하였다 [7].

딥러닝의 활용이 늘어남에 따라 딥러닝 자체에 대한 공격이 등장하기도 하였는데, 많은 취약점을 활용한 공격이 시도되고 있으나 캐시 부채널 공격 (cache side-channel attack)은 물리적 검사 및 피해 시스템과의 직접적인 상호작용을 필요로 하지 않는다는 점에서

그 심각성이 크다고 할 수 있다. 하지만 DNN 역공학 (reverse engineering) 공격은 공격자와 피해 시스템이 메인 메모리를 공유하는 환경에서 DNN 라이브러리의 바이너리 코드 분석에 의존하였으나 운영체제에 의한 메모리 공유 차단 및 라이브러리의 독점 비공개 등으로 인하여 분석이 어렵다는 제약이 있다. Liu와 Srivastava는 캐시 타이밍 부채널 정보를 활용하여 메모리 공유 및 코드 접근 없이도 DNN의 구조를 적확하게 복구하는 GAN (generative adversarial network) 기반의 GANRED 기법을 제시하였다 [8]. GANRED는 Prime+Probe 부채널 공격을 이용하여 메인 메모리를 공유할 필요가 없으며, 공격자 스스로 DNN을 구축하고 부채널로부터 관측된 피해 시스템과 동일한 구조를 가지도록 반복적 업데이트를 수행함으로써 DNN 라이브러리 코드에 접근하지 않고도 피해 모델의 정확한 구조를 특정한다.

3.4. 암호화 및 고립 환경

최근 개인정보보호를 고려한 응용이 다수 등장하면서 종단간 (end-to-end) 클라이언트 측 암호화를 통한 사용자의 데이터 프라이버시 보존 기술 연구가 활발히 이루어지고 있다.

콘텐츠 전송 네트워크 (content delivery network, CDN)로 클라우드 서비스를 활용하면서, 신뢰성 있는 콘텐츠 제공을 위해 대표적 암호통신 프로토콜인 TLS (transport layer security)를 이용하는 환경을 고려할 수 있다. 이를 위해서 사용자와 유효한 연결 설정을 위해 자신을 원본 서버로 인증하여야 하는데, 표준 TLS에서는 서버의 비밀 키에 대한 접근이 필요하므로 위임 기법이 적용되어야 한다. Alber 등은 키 공유가 필요하지 않은 신원 기반 서명 (ID-based signature) 기법을 적용한 단기 위임 기법을 제안하였다 [9]. 전방향 안전성 (forward secrecy)을 제공할 수 있도록 설계된 제안 기법은 서버의 비밀 키 노출로부터도 기존 위임이 계속 유효한 상태로 적용될 수 있으며, 구현을 통하여 낮은 통신 오버헤드를 보임을 증명하였다.

John과 Dirksen은 응용에서 사용되는 자바스크립트 (JavaScript)를 통하여 공격자가 클라이언트 시스템에 대한 향상된 제어가 가능함을 보이며, 웹 기반 클라우드 응용에 그대로 적용되기 어려운 점을 지적하였다. 이를 위하여 사용자와 완벽한 상호운영을 보장하면서 사용자가 암호화한 데이터를 잠재적으로 신뢰할 수 없는 자바스크립트로부터 분리할 수 있는 격리 계층을 제공하여 웹 응용 프로그램 개발을 가능하게 하는 네이티브 클라이언트 측 구성요소 집합인 CryptoMembranes를 제안하였다 [10].

인터넷 검색 엔진을 이용한 사업 모델에서 검색 질의로부터 사용자의 성향을 파악하고 맞춤형 광고를 제공하거나 의사가 원격으로 환자의 유전 데이터를 서비스 제공자에게 질의와 함께 평문 형태로 전달하는 경우에는 환자의 프라이버시가 침해될 수 있다. 따라서 개인 및 데이터 프라이버시 보존을 위해서는 클라우드와 같은 원격 시스템에 저장되는 데이터를 포함하여 검색 질의에 대한 프라이버시가 보존될 필요가 있는데, Bonte와 Iliashenko는 평문의 병렬 연산을 지원하는 하는 패킹 (packing) 기법을 활용한 제한 동형 암호 (somewhat homomorphic encryption, SHE)를 이용하여 검색 문자열의 길이와 무관하게 동일한 곱셈 연산으로 문서 내의 패턴을 검색할 수 있는 기법을 제시하였다 [11]. 연산 깊이를 고정함으로써 선행 연구에 비해 검색 속도를 약 12배 향상시켰으며, 검색 결과를 압축하는 방법을 제공하여 통신 비용 절감을 도모하였다.

클라우드 시스템을 비롯한 컴퓨팅 환경에서는 암호화 및 복호화 키를 알지 못하는 상태에서도 암호문에 대한 연산을 지원하는 동형 암호 (homomorphic encryption) 기법을 이용하여 클라우드 서비스 제공자를 포함한 제3자에게 프라이버시가 보존된 상태에서 연산을 의뢰할 수 있는 환경에 대한 연구가 많은 관심을 받고 있으며, 또한 외부 뿐 아니라 운영체제를 포함한 내부 공격 행위로부터 기밀성 및 무결성 보장을 위하여 신뢰 실행 환경 (trusted execution environment, TEE)을 구축하기 위한 연구도 활발히 진행되고 있다.

3.5. 기타

클라우드 서비스는 기관 또는 개별 사용자가 필요로 하는 충분한 컴퓨팅 자원을 제공할 수 있는 것으로 보이지만, 기하급수적으로 증가하는 데이터 양을 처리하기 위하여 물리적으로 한정된 공간을 효율적으로 사용하기 위하여 데이터 중복제거 (deduplication) 및 변경된 부분만을 별도로 관리하는 델타 인코딩 (delta

encoding)기법 [12]이 적용되고 있다. 또한 클라우드 서비스는 서비스 제공자의 제어 범위를 넘어서는 공개 인터넷을 사용하기에 낮은 지연과 무한정의 대역폭을 제공하기는 어려운 실정이며, 네트워크 끝단의 사용자와 근거리에서 컴퓨팅 자원을 제공하는 엣지 컴퓨팅 (edge computing) 등을 통하여 이동성 및 저지연, 실시간성 등을 보장하기 위한 새로운 패러다임이 등장하기도 하였다.

Ⅳ. 결 론

본 논문에서는 최근 클라우드 서비스에서 발생가능한 보안 취약점 및 이를 해결하기 위한 연구 동향을 살펴보았다. 앞으로는 중앙집중형 클라우드에 대한 보안 취약점 및 대응 방안에서 나아가 개인 시스템에 대한 보안 위협 분석 및 대응의 필요성이 증가하고 있다.

Gartner는 '네트워크 보안의 미래가 클라우드에 있다'고 언급하며, 앞으로의 네트워크 및 보안 서비스 디자인은 중앙집중형의 데이터 센터가 아닌 사용자 및 개별 장치에 집중되어 통합 클라우드 제공 보안 접근 서비스가 필요함을 역설하였다 [13]. 이는 엣지 컴퓨팅 (edge computing) 환경에서 사용자, 장치, 응용, 서비스 및 데이터가 중앙 클라우드 내부보다 외부에 더 많은 요구사항이 필요하고, 암호화된 트래픽의 복호화 및 검사를 위한 Security-as-a-Service 기능이 클라우드 제공 보안 접근 엣지 (secure access service edge, SASE)으로의 통합 수요가 증가할 것으로 예상하고 있다.

사용자는 보안 취약점이 발견되고 개선되는 과정에서 서비스 수준 협약 (service level agreement, SLA)에 사용자 데이터에 대한 기밀성 및 무결성에 대한 보장 범위를 명확히 확인할 필요가 있을 것이다. Dropbox에서는 계열사 및 신뢰할 수 있는 협력업체에게 데이터에 대한 접근 및 저장, 스캔을 할 수 있는 권한을 부여하도록 규정하고 있으며 [14], Google에서도 사용자 콘텐츠의 호스팅, 복제, 배포, 전달, 사용, 게시 및 공개 표시에 대한 권한을 명시하고 있다 [15]. 최근에는 유럽 개인정보보호법 (General Data Protection Regulation) 및 국내 개인정보보호법/정보통신망법/신용정보법 (데이터 3법)에 대한 개정을 통하여 클라우드 및 사물인터넷 환경에서 안전한 데이터 관리를 위한 규정이 마련되면서 개인정보보호를 위한 노력이 이루어지고 있으나, 악의적 행위로부터의 대응 방안 및 개선책 마련에 대한 연구는 지속적으로 수행될 필요가 있을 것이다.

참 고 문 헌

[1] NIST, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, 2020

[2] THALES, "2020 Thales Data Threat Report Asia-Pacific Edition," https://cpl.thalesgroup.com/sites/default/files/2020-09/DTR_2020_APAC_infographic_KR.pdf, 2020 (accessed on 23 Nov. 2020)

[3] M.G. Jaatun, "Architectural Risk Analysis in Agile Development of Cloud Software," *IEEE International Conference on Cloud Computing Technology and Science*, pp. 295-300, Dec. 2019

[4] S. Shringarputale, P. McDaniel, K. Butler, T.L. Porta, "Co-residency Attacks on Containers are Real," *ACM Cloud Computing Security Workshop*, pp. 53-66, Sep. 2020

[5] Y. Qin, S. Gonzalez, K. Angstadt, X. Wang, S. Forrest, R. Das, K. Leach, W. Weimer, "MARTINI: Memory Access Traces to Detect Attacks," *ACM Cloud Computing Security Workshop*, pp. 77-90, Sep. 2020

[6] B.Z.H. Zhao, M.A. Kaafar, N. Kourtellis, "Not one but many Tradeoffs: Privacy Vs. Utility in Differentially Private Machine Learning," *ACM Cloud Computing Security Workshop*, pp. 15-26, Sep. 2020

[7] C. Zhang, X. Costa-Perez, P. Patras, "Tiki-Taka: Attacking and Defending Deep Learning-based Intrusion Detection Systems," *ACM Cloud Computing Security Workshop*, pp. 27-39, Sep. 2020

[8] Y. Liu, A. Srivastava, "GANRED: GAN-based Reverse Engineering of DNNs via Cache Side-Channel," *ACM Cloud Computing Security Workshop*, pp. 41-52, Sep. 2020

[9] L. Alber, S. More, S. Ramacher, "Short-Lived Forward-Secure Delegation for TLS," *ACM Cloud Computing Security Workshop*, pp.

119-132, Sep. 2020

[10] M. Johns, A. Dirksen, “Towards Enabling Secure Web-Based Cloud Services using Clint-Side Encryption,” *ACM Cloud Computing Security Workshop*, pp. 67-76, Sep. 2020

[11] C. Bonte, I. Iliashenko, “Homomorphic String Search with Constant Multiplicative Depth,” *ACM Cloud Computing Security Workshop*, pp. 105-117, Sep. 2020

[12] E. Henziger, N. Carlsson, “Delta Encoding Overhead Analysis of Cloud Storage Systems using Client-side Encryption,” *IEEE International Conference on Cloud Computing Technology and Science*, pp. 183-190, Dec. 2019

[13] N. MacDonald, L. Orans, J. Skorupa, “The Future of Network Security Is in the Cloud,” Gartner, https://www.gartner.com/doc/reprints?id=1-2445LMXN&ct=200908&st=sb, 30 Aug. 2019 (accessed on 23 Nov. 2020)

[14] Dropbox, Inc., “Dropbox Terms of Service,” https://www.dropbox.com/terms, 25 Jul. 2019 (accessed on 23 Nov. 2020)

[15] Google, “Privacy & Terems,” https://policies.google.com/terms, 31 Mar. 2020 (accessed on 23 Nov. 2020)

〈저자소개〉

구 동 영 (Dongyoung Koo)

종신회원

2009년 2월 : 연세대학교 컴퓨터.산업공학과 졸업

2012년 2월 : 한국과학기술원 전산학과 석사

2016년 2월 : 한국과학기술원 전산학부 박사

2016년 3월~2018년 3월 : 고려대학교 정보대학 컴퓨터학과 연구교수

2017년 4월~현재 : 한성대학교 기계전자공학부 조교수

<관심분야> 정보보호, 암호 응용, 클라우드 보안, 네트워크 보안