특집 04

클라우드 스토리지 보안 기술 동향

황우민 · 김성진 · 김형천 (국가보안기술연구소)

목 차

1. 서 론

클라우드 컴퓨팅은 주문형 셀프 서비스, 광대역 네트워크 접근, 자원 공동관리, 빠른 탄력성, 측정 가능한 서비스의 특성을 갖는 차세대 컴퓨팅 구조[58]로서 가용성, 유연한 확장성, 높은 접근성 등의 장점을 앞세워 빠르게 확산되고 있다. 사용자들은 클라우드에 저장된 자신의 데이터를 위치에 구애받지 않고 클라우드로의 네트워크 연결만으로 접근할 수 있으며 스토리지 관리 부담을 줄일 수 있고 필요한 만큼 사용하고 그에 대한 비용만을 지불할 수 있기 때문에 비용 절감 효과를 얻을 수 있는 장점이 있다. 하지만 클라우드 환경에서는 다수의 사용자가 중앙 집중화된 컴퓨팅 환경을 공유하기 때문에 저장된 데이터를 보호하기 위한 기본적인 데이터 안전성 확보와 자료 유출 방지, 복구, 모니터링 및 통합 인증, 접근 권한 관리 기술 등 다양한 보안 요구사항을 만족시킬 수 있는 확장성 있는 저장기술이 필요하다.

주요 국제 기관들에서는 이러한 클라우드 컴퓨팅 환경에서 발생할 수 있는 보안 위협에 대해서 분류, 분석하고 보안 요구사항들을 도출하는 작업을 수행하고 있다. CSA(Cloud Security Alliance)는 클라우드 환경에서의 보안 위협을 12가지로 분류하여 분석하였고[1], ITU-T에서는 X.1601에서 클라우드 컴퓨팅 보안 위협을[7], ENISA는 17종류의 사이버 위협들을 분류하고 각각에 대해서 분석하였다[8].

본 고에서는 이들 중 클라우드 스토리지의 보안과 관련된 네 가지 위협, 즉, 데이터 유출, 유실, 악의적인 서비스 제공자 위협 및 공유 기술 문제를 간략히 정리하고 클라우드 스토리지와 관련된 보안 기술 연구 동향에 대하여 기술한다.

2. 클라우드 스토리지

클라우드 스토리지는 클라우드 환경에서 데이터가 저장되는 논리적 스토리지 연합체로써 다

수의 분산된 저장 장치를 연결하여 저장 공간을 생성함으로써 클라우드 사용자로 하여금 데이터를 저장하고 접근할 수 있도록 관리하는 스토리지로 정의된다. 이러한 클라우드 스토리지에 사용되는 기술의 주요 예로써 HDFS, Swift, Glory-FS, OwFS, GlusterFS, NFS/CIFS, 상용 서비스의 예로써 Google Cloud Storage, Amazon S3 등이 있다.

HDFS(Hadoop Distributed File System)[10,11]는 대량의 자료 처리를 위한 분산 응용 프로그램을 지원하는 Hadoop 분산처리 프레임워크의 분산 파일 시스템으로 커버로스(Kerberos) 및 토큰 시스템을 이용한 인증 및 접근 제어를 사용하며 이와 유사한 Glory-FS[9]도 데이터 접근 제어 및 암/복호화를 지원한다.

Swift[12]는 OpenStack의 object storage 시스템으로서 분산된 상용 스토리지 자원들을 이용하는 스토리지 서비스로 오류를 대비하여 객체들을 클러스터 내 저장장치에 중복되어 분산 저장하고 데이터의 무결성을 제공한다. 안정화 버전에서는 Keystone을 이용한 권한관리만을 제공하지만 개발 버전에서는 AES 암호화를 적용 중이다. 네이버가 개발하여 사용하고 있는 대규모 분산 파일 시스템인 OwFS(Owner-based File System)[13]는 파일에 대한 암호화를 적용하고 있고 GlusterFS[14]는 파일의 내용에 대한 암호화 기능과 함께 데이터로의 접근시 사용자 인증 기능도 함께 제공하고 있다. NFS[15]/CIFS는 네트워크를 통해 다른 호스트에 있는 파일을 공유해서 사용할 수 있는 분산 파일 시스템으로 로컬 파일 시스템과 동일한 기능을 제공하므로 응용 프로그램의 구동시 로컬 파일 시스템과 분산 파일 시스템을 구별하지 않는다. NFS는 version 4에서 클라이언트/서버 인증과 Kerberos를 통해서 데이터 무결성/기밀성을 제공한다.

이외에도 상용 서비스들, 예를 들어 Google Cloud Storage[5]는 모든 데이터에 대해 쓰기 작업이 진행되기 전 256bit AES 암호화를 강제하는 정책을 적용중이고 Amazon S3[39]는 클라이언트/서버측에서 암호화를 지원하여 서비스 사용자 및 제공자 측면에서의 데이터 암호화를 제공한다.

이러한 예에서 볼 수 있듯 대다수의 클라우드 스토리지가 데이터 암호화 및 접근 사용자의 인증을 제공하지만 저장 데이터의 대형화를 수용하기 위해 각 구성 요소들이 네트워크화되고 있어 이에 적합한 암호화 기술 및 접근 제어 기술의 필요성이 증가하고 있다. 하지만 대용량 데이터 처리에의 암호화/접근 제어 기술의 적용은 성능 저하를 야기할 가능성이 높으므로 클라우드 스토리지에 저장되는 데이터를 효율적으로 보호하기 위해서는 연산 효율적 암호화 기술의 개발 및 적용이 필요할 뿐만 아니라 보다 정확한 위협의 식별 및 이에 따른 데이터로의 접근 통제 및 보호를 위한 기술 개발, 저부하 데이터 흐름 모니터링 기술 등의 연구가 필요하다.

3. 클라우드 스토리지 보안 기술 연구 동향

3.1 보안 위협 요소

클라우드 컴퓨팅과 관련하여 2016년도에 CSA가 갱신한 12가지 위협 요소 분류, ITU-T X.1601[7]에서 분류한 클라우드 컴퓨팅 보안 위협, ENISA에서 분류한 17가지 사이버 위협들[8] 중에서 클라우드 스토리지와 관련성이 높은 것들을 [6]에서 식별한 과거의 보안 위협을 참조하여 CSA의 용어를 기준으로 분류하면 1) 데이터 유출; 2) 악의적인 서비스 제공자; 3) 데이터 유실;

4) 공유 기술 문제의 네 가지로 나타낼 수 있다.

3.1.1 데이터 유출

2016년도에 갱신된 클라우드 스택[2]의 보안 부분에도 본 위협에 대한 대비가 요소 기술의 하나로 포함되어 있는 데이터 유출 위협은 허가받지 않은 사용자의 데이터 생성, 접근, 사용에 대한 통제가 적절하게 이루어지지 않을 경우에 존재한다. 공유를 기반으로 하는 클라우드 환경에서 저장된 데이터는 내부의 임의 사용자, 같은 스토리지를 사용하는 임의의 가상 머신, 네트워크를 통한 접근자 등에 의해서 접근될 수 있다. 특히 IaaS (Infrastructure as a Service) 및 PaaS (Platform as a Service) 서비스 모델을 사용하는 환경은 기반이 되는 클라우드 인프라에 대한 접근성이 높은 특성을 가지므로 유출 위협으로부터 데이터를 보호하기 위한 추가적인 노력이 필요하다. 예를 들어, 금융권 및 의료 관련 데이터와 같이 극도의 기밀성을 유지해야 하는 데이터의 경우 암호화 및 높은 접근 통제 수준을 적용해야 한다.

3.1.2 악의적인 서비스 제공자

기존 내부자 보안은 기업 내부에 통제권이 있기 때문에 높은 통제 수준을 유지할 수 있었지만 기업 내부 데이터들이 클라우드 환경에 존재하는 경우 이를 관리하는 통제권이 클라우드 서비스 제공자에게 있게 된다. 기업은 자신의 데이터를 관리하는 사람에 대한 통제권이 약해지게 될 수 밖에 없어 클라우드 서비스 제공자 내부의 악의적인 관리자가 기업의 데이터에 대한 접근 시이를 통제하고 모니터링할 수 있는 방안이 필요하며 이러한 보안 정책이 이행되고 있는지를 관리, 감독할 수 있어야 한다.

3.1.3 데이터 유실

데이터 유실 위협은 2009년도 MS 사이드킥 사고[3], 2011년도 구글 Gmail 삭제 사고, 2015년 구글 데이터 유실 사고[4] 에서와 같이 실존하면서도 지속적으로 발생하는 보안 위협이다. 2014년도 6월에는 온라인 호스팅 업체인 Code Spaces가 해킹에 의한 사용자 데이터의 파괴로 서비스를 종료한 사례[1]에서도 볼 수 있듯 데이터 손실에 대비하기 위한 다양한 방법이 존재하지만 이들이 정상적으로 동작하지 않거나 대비하지 못한 유형의 원인에서 발생하는 위협일 경우 큰 피해가 발생할 수 있다. 따라서 다양한 유형의 원인으로부터 야기되는 손실에 대비할 수 있는 안정적이면서도 효율적인 저장기술이 필요하다.

3.1.4 공유 기술 문제

클라우드의 확정성은 클라우드 인프라를 공유함으로써 달성된다. 저장 공간을 비롯한 공유되는 자원 상에서 이용자들에 대한 서비스가 이루어지기 때문에 가상 환경의 바탕이 되는 공유 자원 상에서 강력한 격리가 이루어지지 않을 경우 임의의 사용자가 다른 사용자의 데이터에 접근한 수 있는 상황이 발생할 수 있다. 클라우드 서비스 제공자는 적절한 수준의 공유 기술을 적용함으로써 효율성과 확장성을 보장하는 동시에 물리적/논리적 격리 기술을 적용하여 공유 기술에 의한 보안 위협을 방지해야 한다.

이외에도 [6]에서는 서비스 가용 여부를 저장장치 가상화 시스템 보안 위협의 하나로 보고 사고 모니터링 및 사고 대응을 보안 요구사항의 하나로 제안하고 있다.

3.2 스토리지 보안 기술 동향

이전 절에서 언급한 보안 위협에 대응하기 위해서 다양한 기술에 대한 연구가 진행되고 있다. 클라우드 컴퓨팅 환경에서의 스토리지 보안 기술은 크게 사용자 측면의 클라우드 단말 보안 기술과 서비스 제공자 측면의 클라우드 서비스 보안 기술로 나눌 수 있다. 사용자 단말 측면에서의 스토리지 보안 기술에는 단말 스토리지 및 저장 데이터의 무결성 보장 기술 및 저장 자원 또는 데이터로의 접근을 제어하기 위한 사용자 인증, 인가 및 접근 제어 기술 등이 포함된다. 제공자 측면에서 적용 가능한 클라우드 스토리지 보안 기술은 클라우드 서비스의 제공 형태에 따라 다시 인프라(IaaS), 플랫폼(PaaS), 서비스(SaaS) 영역에서의 스토리지 보안 기술로 구분할 수 있다.

사용자 단말 보안 측면에서는 NIST(National Institute of Standards and Technology)가 사용자 단말 스토리지 암호화, 암호 키 관리 및 사용자 인증에 대한 가이드라인 문서[16]를 발간하여 주요 주제로 단말 무결성과 데이터 접근 제어 등을 다루었다. 단말에 저장된 플랫폼의 무결성을 보장하기 위해 단말의 안전한 부팅[56]을 지원하는 기능을 제공하기도 하며 단말에서의 데이터 유출 방지를 위한 ARM TrustZone을 이용한 모바일 클라우드 스토리지 서비스에서 데이터 유출 방지 연구[40]와 사용자 단말에서의 접근 제어 기술[48] 등은 ARM TrustZone과 같은 하드웨어 지원 기능을 활용하여 플랫폼 무결성 검증 및 파일 암복호화 기능을 안전하게 제공한다. 이외에도 저장된 데이터의 완전 삭제 기술[59] 및 저장된 데이터로의 접근을 포함하는 데이터의 이동 흐름에 대한 모니터링 및 기록을 위해 정보 흐름 추적 기술(Information Flow Tracking)[26,27]과 같은 데이터 흐름 모니터링 기술들이 데이터에 대한 접근 제어, 로깅 및 감사 추적을 위한 용도로 연구되고 있다.

인프라 형태의 클라우드 서비스(IaaS) 제공자에서의 스토리지 보안 기술은 주로 기반 보호 기술로써 자료유출 방지 및 스토리지 암호화 기술, 안전한 데이터 중복 제거 등의 연구가 활발하게 이루어지고 있다. 자료 유출 방지(DLP) 기술은 기밀 정보에 대한 허가받지 않은 접근, 사용, 전송을 막기 위한 기술 또는 심층 컨텐츠 분석을 통해 사용, 전송중이거나 변경 없는 데이터를 중앙 정책에 기반하여 확인, 모니터링, 보호하는 기술로 정의되며[49] 산업계에서도 많은 제품이 출시되어 있다. 최근 학계에서는 스토리지 수준 IDS(Intrusion Detection System)[34,35,36], 데이터 labeling, 데이터 필터[28] 등의 연구들이 이루어지고 있다.

스토리지 데이터의 암호화를 위해 IEEE P1619[31]는 블록 기반 스토리지 장치에서의 데이터 암호화 보호에 대한 표준을 제시하였으며 데이터 유실 및 유출과 관련된 식별, 규정, 접근 제어 및 관련 속성과 관련해서는 SAML, X.509 인증 등이 사용되고 있다[30]. 일반적인 스토리지 암호화는 전체 디스크 암호화[32,33], 가상 디스크 암호화 및 볼륨 암호화[47], 그리고 일반적으로 가장 널리 사용되는 파일/폴더 암호화등이 있다. 이외에도 다양한 클라우드용 경량 암호화 기술[52,53]이 연구되고 있으며 산업계에서도 구글은 2013년부터 public cloud 서비스의 스토리지에 저장되는 모든 데이터를 자동 암호화[5]하고, 이외에도 클라우드 서비스 제공자들은 사용자 데이터의 암호화 기능을 기본/옵션으로 제공하고 있다.

중복 제거(Deduplication) 기술은 클라우드 저장 공간 내 중복된 데이터에 대한 저장 공간 절감 및 통신 부담을 덜기 위해 적용되나 보안에

대한 고려가 없을 경우 side-channel attack[49]에 의해 데이터의 저장 여부를 공격자에게 노출시키거나 암호화에 의해 중복 제거가 의미없게 되는[50] 문제가 있다. 최근에는 사용자 단말[24], 클라우드 서비스 제공자[21,22,25,50] 측면에서 보안성을 고려한 저장된 데이터에 대한 중복 제거 기술들이 연구되고 있다.

이외에도 스토리지 무결성 보장과 관련하여 클라우드 환경에서 사용되는 데이터 무결성 검증[37,38,71] 기법 등이 연구되고 있으며 감사 기법[41,42,43,44]들도 제안되고 있다.

플랫폼 형태의 서비스 제공자 측면에서의 스토리지 보안 기술은 분산 데이터의 접근 제어 및 사용자 데이터 보호와 관련된 연구들이 이어지고 있다. 특히 클라우드 스토리지에 저장된 대용량 정보를 암호화된 상태로 저장하면서 검색 등 필요한 작업을 수행할 수 있도록 하는 검색 가능 암호[45,46]가 빅데이터 분야를 포함하여 연구되고 있다.

클라우드 서비스 제공자 측면에서의 스토리지 보안 기술은 사용자 데이터 보호가 주를 이루며 데이터 권한 관리 및 기밀성 보장을 위한 데이터 암호화[54,55] 등이 연구되고 있다.

또한 서비스 유형에 관계없이 저장된 데이터의 복구를 용이하게 하기 위한 기술[57,67], 및 정상적으로 삭제되거나 가입 해지된 사용자의 데이터에 대한 클라우드 스토리지로부터의 완전 삭제 기술이 저장된 데이터의 복구를 어렵게 하는 의미로 통용되어 클라우드 안티 포렌식 기술[69]과 연계되어 연구되고 있다. 그리고 스토리지 저장 데이터로의 입출력과 관계된 보안 감사 및 이벤트 관리/모니터링과 관련하여 스토리지 저장 데이터로의 입출력에 대한 모니터링[18,19,20] 기법들도 연구되고 있다.

클라우드 환경에서의 보안 사고에 대한 대응 및 조사와 관련하여 디지털 포렌식을 지원할 수 있는 스토리지 관련 기술 또한 중요한 이슈로 부각되고 있다. 이와 관련하여 [60,61,64,66]에서는 클라우드 환경에서의 포렌식 조사를 위한 기술적 이슈들을 다루었으며 로깅 기반 포렌식 기술[62,63,68] 및 증거 추적 및 재구성을 위한 포렌식 프레임워크[65], 클라우드 환경에서의 포렌식 기술[70] 등이 제안되었다.

4. 결 론

클라우드 컴퓨팅 환경은 증가하는 데이터의 양과 늘어나는 사용자 수에 따라 다양한 보안 위협에 노출되고 있으며 여러 구성 요소들 중에서도 클라우드 스토리지 시스템은 사용자의 데이터 유출, 유실, 악의적인 서비스 제공자로부터의 공격, 그리고 클라우드 효율성을 위한 공유 기술에서 파생되는 문제와 같은 데이터의 중앙집중화에 따른 보안 위협을 받을 수 있기 때문에 보안상의 대비가 반드시 이루어져야 한다.

본 고에서는 기존에 분류되었던 클라우드 스토리지와 관련된 보안 위협의 분류들을 갱신하고, 해당 보안 위협과 관련된 연구 동향을 알아보았다. 이후, 이를 바탕으로 클라우드 스토리지 시스템의 보안 위협에 대응하는 연구를 진행할 계획이다.

참 고 문 헌

[1] CSA Top Threats Working Group, “The Treacherous 12: Cloud Computing Top Threats in 2016,” Cloud Security Alliance (CSA), Feb 2016.

[2] 클라우드컴퓨팅 연구조합, 차세대컴퓨팅학회, “2015 클라우드 컴퓨팅 기술 스택,” 2016.01
[3] 정성재, 배유미, “클라우드 보안 위협요소와 기술 동향 분석,“ 보안공학연구논문지, 2013.04
[4] Google Compute Engine Incident #15056, https://status.cloud.google.com/incident/compute/15056#5719570367119360, (2016.07.06)
[5] Dave Barth, “Google Cloud Storage now provides server-side encruption,” https://cloudplatform.googleblog.com/2013/08/google-cloud-storage-now-provides.html, Google Cloud Platform Blog (2016.07.06)
[6] 주정호 외, “클라우드 컴퓨팅 보안 위협에 대처한 저장장치 가상화 시스템 보안 요구 사항 제안,” 보안공학연구논문지 Vol.11, No.6, 2014
[7] ITU-T Study Group 17, “Recommendation ITU-T X.1601 Security framework for cloud computing,” 2015.10, available on http://handle.itu.int/11.1002/1000/12613
[8] ENISA, “ENISA threat Landscape 2015 (ETL 2015),“ 2016.01, available on https://www.enisa.europa.eu/publications/etl2015
[9] 김홍연 외, "GLORY-FS: 대규모 인터넷 서비스를 위한 분산 파일 시스템." The Journal of The Korean Institute of Communication Sciences, 30.4 (2013.3): 16-22.
[10] Hadoop Project, http://hadoop.apache.org
[11] K. Shvachko et al., “The Hadoop Distributed File System.” In Proceedings of the 2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST) (MSST '10). IEEE Computer Society, Washington, DC, USA, 1-10.
[12] OpenStack Swift, http://www.openstack.org
[13] 김진수, 김태웅, “OwFS: 대규모 인터넷 서비스를 위한 분산 파일 시스템,” 정보과학회지 27권 5호, 2009.05.
[14] GlusterFS, “Open source, distributed file system,” http://www.gluster.org, March 2013.
[15] IETF, RFC5661, Network File System (NFS) Version 4 Minor Version 1 Protocol, Jan. 2010
[16] K Scarfone et al., “Guide to Storage Encryption Technologies for End User Devices,” NIST Special Publication 800-111, Nov. 2007.
[17] 박정수, 배유미, 정성재. (2013.5). 클라우드 컴퓨팅을 위한 클라우드 스토리지 기술 분석. 한국정보통신학회논문지, 17(5), 1129-1137.
[18] Xuxian Jiang et al., “Stealthy malware detection and monitoring through VMM-based “out-of-the-box” semantic view reconstruction,“ ACM Trans. Inf. Syst. Secur.13, 2, Article 12 (March 2010), 28 pages.
[19] C. Benninger et al., “Maitland: Lighter-weight VM introspection to support cyber-security in the cloud,” CLOUD’12, pages 471-478, June 2012.
[20] Wolfgang Richter, “Agentless cloud-wide monitoring of virtual disk state,” In Proceedings of the 2014 workshop on PhD forum (PhD forum '14). ACM, New York, NY, USA, 15-16.
[21] W. Richter et al., “Agentless Cloud-Wide Streaming of Guest File System Updates,” IC2’14, IEEE Computer Society, Washington, DC, USA.
[22] P. Puzio et al., “ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage.” 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, 2013, pp. 363-370.
[23] J. Stanek et al., "A secure data deduplication scheme for cloud storage." International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014.
[24] N. Kaaniche and M. Laurent, "A Secure Client Side Deduplication Scheme in Cloud

Storage Environments," 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), Dubai, 2014, pp. 1-7.
[25] Mark W. Storer et al., "Secure data deduplication," In Proceedings of the 4th ACM international workshop on Storage security and survivability (StorageSS '08). ACM, New York, NY, USA, 1-10.
[26] Man-Ki Yoon et al., "PIFT: Predictive Information-Flow Tracking," In Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '16). ACM, New York, NY, USA, 713-725.
[27] C. Wang and Shiuhpyng Winston Shieh. "SWIFT: Decoupled System-Wide Information Flow Tracking and its Optimizations." Journal of Information Science and Engineering 31.4 (2015): 1413-1429.
[28] Christos Gkantsidis et al., "Rhea: automatic filtering for unstructured cloud storage," In Proceedings of the 10th USENIX conference on Networked Systems Design and Implementation (nsdi'13), USENIX Association, Berkeley, CA, USA, 343-356.
[29] Dongyoung Koo et al., "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage," Comput. Electr. Eng. 39, 1 (January 2013), 34-46.
[30] 허의남, "퍼스널 클라우드 보안 기술과 프라이버시," TTA 저널 no.139, 2012, 65-69.
[31] IEEE Security in Storage Working Group, "IEEE P1619/D16 Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices," IEEE Computer Society Committee, May 2007.
[32] E. Casey and Gerasimos J. Stellatos, "The impact of full disk encryption on digital forensics." ACM SIGOPS Operating Systems Review42.3 (2008): 93-98.
[33] E. Casey et al. "The growing impact of full disk encryption on digital forensics," Digital Investigation 8.2 (2011): 129-134.
[34] A. Bacs et al., "Slick: an intrusion detection system for virtualized storage devices," In Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC '16). ACM, New York, NY, USA, 2033-2040.
[35] Adam G. Pennington et al., "Storage-Based Intrusion Detection," ACM Trans. Inf. Syst. Secur. 13, 4, Article 30 (December 2010), 27 pages.
[36] Anjo Vahldiek-Oberwagner et al., "Guardat: enforcing data policies at the storage layer," In Proceedings of the Tenth European Conference on Computer Systems (EuroSys '15). ACM, New York, NY, USA, , Article 13, 16 pages.
[37] 은하수 외, "Outsourced Storage Auditing Scheme using Coefficient Matrix," 정보처리학회논문지 2.11 (2013): 483-488.
[38] 김태연, 조기환, "클라우드 컴퓨팅에서 동적 데이터 무결성을 위한 개선된 감사 시스템," 한국정보통신학회논문지 Vol.19, No.8, (2015.08): 1818-1824.
[39] Amazon S3, "Protecting Data Using Encryption," http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html (2016,07,06)
[40] 신재복 외, "클라우드 스토리지 서비스를 위한 ARM TrustZone 기반의 안전한 데이터 관리 기법," 대한임베디드공학회 추계학술대회, 2012. 11. 85-88.
[41] 백목련 외, "안전한 클라우드 스토리지를 위한 프라이버시 보장 자체 인증 공공 감사," 정보과학회논문지, 43(4), 497-508.
[42] 권오민, 윤현수, "클라우드 데이터 무결성 검증 방법 조사," 한국정보과학회 학술발표논문집, 2013.6, 689-691.
[43] 신수연, 권태경, "손상 클라우드 식별 가능한 다

중 클라우드 일괄 감사 기법에 관한 연구," 정보보호학회논문지 25(1), 2015.2, 75-82.
[44] C. Wang et al., "Privacy-Preserving Public Auditing for Secure Cloud Storage," in IEEE Transactions on Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
[45] M. Bakhtiari et al., "Secure Search Over Encrypted Data in Cloud Computing," Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on, Kuching, 2013, pp. 290-295.
[46] C. Liu et al., "Efficient Searchable Symmetric Encryption for Storing Multiple Source Data on Cloud," Trustcom/BigDataSE/ISPA, 2015 IEEE, Helsinki, 2015, pp. 451-458.
[47] K. Beer and R. Holland, "Securing Data at Rest with Encryption," Amazon Web Services, Nov. 2013.
[48] 신재복 외, "모바일 클라우드 스토리지 서비스에서의 데이터 보안을 위한 데이터 접근 제어 및 보안 키 관리 기법," 대한임베디드공학회논문지 8(6), 303-309.
[49] S. Alneyadi et al., "A survey on data leakage prevention systems," Journal of Network and Computer Applications 62, 2016, 137-152.
[50] D. Harnik et al, "Side channels in cloud services: Deduplication in cloud storage." IEEE S&P, 8(6) 2010, 40-47
[51] S. Keelveedhi et al., "DupLESS: server-aided encryption for deduplicated storage." 22nd USENIX Security Symposium (USENIX Security 13). 2013.
[52] S. Matsuda and S. Moriai, "Lightweight Cryptography for the Cloud: Exploit the Power of Bitslice Implementation," Cryptographic Hardware and Embedded Systems (CHES), 2012, 408-425
[53] S. Belguith et al., "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm," Eleventh International Conference on Autonomic and Autonomous Systems, 2015.
[54] Y. Chou et al., "Enforcing confidentiality in a SaaS cloud environment," Telecommunications Forum (TELFOR), 2011, 90-93.
[55] S. Rehman and R. Gautam, "Research on ACcess Control Techniques in SaaS of Cloud Computing," Security in Computing and Communications, Springer, 2014, 92-100.
[56] R. Wilkins and B. Richardson, "UEFI Secure Boot in Modern Computer Security Solutions," UEFI Forum, Sep. 2013.
[57] O. Khan et al., "Rethinking Erasure Codes for Cloud File Systems: Minimizing I/O for Recovery and Degraded Reads," USENIX FAST, 2012.
[58] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[59] Xingjie Yu et al., "Remotely wiping sensitive data on stolen smartphones," In Proceedings of the 9th ACM symposium on Information, computer and communications security (ASIA CCS '14). ACM, New York, NY, USA, 537-542.
[60] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, Oakland, CA, 2011, pp. 1-10.
[61] S. Alqahtany et al., "Cloud Forensics: A Review of Challenges, Solutions and Open Problems," Cloud Computing (ICCC), 2015 International Conference on, Riyadh, 2015, pp. 1-9.
[62] S. Zawoad et al., "Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service," in IEEE Transactions

on Dependable and Secure Computing, vol. 13, no. 2, pp. 148-162, March-April 1 2016.
[63] T. Sang, "A Log Based Approach to Make Digital Forensics Easier on Cloud Computing," Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on, Hong Kong, 2013, pp. 91-94.
[64] A. K. Mishra et al., "Cloud Forensics: State-of-the-Art and Research Challenges," Cloud and Services Computing (ISCOS), 2012 International Symposium on, Mangalore, 2012, pp. 164-170.
[65] S. Almulla et al., "A Distributed Snapshot Framework for Digital Forensics Evidence Extraction and Event Reconstruction from Cloud Environment," 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, 2013, pp. 699-704.
[66] V. M. Katilu et al., "Challenges of Data Provenance for Cloud Forensic Investigations," Availability, Reliability and Security (ARES), 2015 10th International Conference on, Toulouse, 2015, pp. 312-317.
[67] 남궁재웅 외, “포렌식 관점의 파티션 복구 기법에 관한 연구,” Journal of The Korea Institute of Information Security & Cryptology, 23(4), 2013.08, 655-665.
[68] S. Khan et al., “Cloud Log Forensics: Foundations, State of the Art, and Future Directions,” ACM Computing Syrveys 49(1), Feb. 2016.
[69] NIST Cloud Computing Forensic Science Working Group IT Laboratory, “Draft NISTIR 8006, NIST Cloud Computing Forensic Science Challenges,” NIST, 2014.
[70] 정일훈 외, “IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구,“ 정보보호학회논문지 21(6), 2011.12, 55-65.
[71] 김등화 외, “사설 클라우드 환경에서 수집된 VM 데이터의 무결성 입증과 관련 포렌식 도구의 신뢰성 검증,” 정보보호학회논문지 23(2), 2013.4, 223-230.

저 자 약 력

황 우 민

이메일 : wmhwang@nsr.re.kr

- 2015년 한국과학기술원 전기및전자공학과 (박사)
- 2014년~현재 국가보안기술연구소 연구원
- 관심분야 : 클라우드, 고성능 컴퓨팅, 시스템 보안, 가상화 보안

김 성 진

이메일 : ksj1230@nsr.re.kr

- 2010년 포항공과대학교 정보통신학 (석사)
- 2010년~현재 국가보안기술연구소 선임연구원
- 관심분야 : 컴퓨터 보안, 악성코드 분석

김 형 천

이메일 : khche@nsr.re.kr

- 2011년 고려대학교 정보보호대학원 (박사)
- 2001년~현재 국가보안기술연구소 책임연구원
- 관심분야 : 클라우드 보안, 컴퓨터 보안