정 보 보 호 학 회 지
제 32 권 제2호, 2022. 4

디지털 포렌식 관점에서 클라우드 스토리지 분석 연구 동향

서 승 희*, 김 주 은*, 이 창 훈**

요 약

클라우드 스토리지는 다양한 리소스에서 인터넷을 통해 데이터를 저장하고 접근하는 형태의 데이터 스토리지를 말한다. 클라우드 스토리지는 서비스 접근성, 용량 조절의 용이성이 높아 꾸준히 사용자가 증가해왔다. 특히 모바일 기기와 연동하여 자동 동기화함으로써 사용자와 관련한 다양한 데이터가 실시간으로 업·다운로드 된다. 이에 따라 클라우드 스토리지에는 디지털 포렌식 관점에서 특정 사실을 증명하거나 사건의 실마리가 되는 중요한 단서가 저장되어 있을 가능성이 크다. 따라서, 본 논문에서는 클라우드 스토리지의 정의와 종류를 살펴보고 디지털 포렌식 관점에서 클라우드 스토리지의 데이터 수집 및 분석 기술에 관한 연구 동향을 분석한다. 또한, 현재 클라우드 스토리지 데이터 수집 기술의 한계를 분석하고 향후 연구 방향에 관해 논의한다.

Ⅰ. 서 론

클라우드 스토리지는 최종 사용자가 컴퓨터, 스마트폰, 태블릿 등 다양한 리소스에서 인터넷을 통해 데이터를 저장하고 엑세스하는 형태의 데이터 스토리지를 말한다. 클라우드 스토리지 서비스 제공업체는 솔루션을 통해 이러한 데이터 스토리지를 관리·운영하고 데이터의 백업, 복구, 공동작업 등의 서비스를 제공하고 있다.

클라우드 스토리지 서비스는 접근 수단, 위치 등의 제약이 없는 손쉬운 접근성과 용량 조절의 유연성, 데이터 관리의 안정성 등을 보장함에 따라 서비스 이용률은 꾸준히 증가해왔다. 정보통신정책연구원(KISDI)의 국내 '클라우드 서비스 이용 추이 및 현황' 보고서에 따르면, 국내 클라우드 서비스 이용률은 2012년 약 5%에서 약 20%로 약 4배 증가하였다[1].

특히, 모바일 기기는 카메라 성능이 향상됨에 따라 미디어 파일의 크기가 증가하고 있으나 저장 공간의 제약이 많고 용량 조절이 어려워 데이터 저장·백업을 위해 대부분 클라우드 스토리지 서비스를 이용한다. 또한, 편리한 백업을 위해 자동으로 사진이 업·다운로드되는 동기화 기능을 사용하므로, 디지털 포렌식 관점에서 클라우드 스토리지에는 특정 사실을 증명하거나 사건의 실마리가 되는 단서가 저장되어 있을 가능성이 크다.

실제로 2019년 9월 광주 서구에서는 27세 남성이 버스 정류장에서 20대 여성의 신체 일부를 촬영한 사실을 부인하였으나, 클라우드 스토리지에 자동 동기화된 해당 여성을 촬영한 60여 개의 영상이 적발되어 불법 촬영 및 성적 촬영물 소지에 따른 성폭력범죄의 처벌 등에 관한 특례법 위반 혐의로 입건된 바 있다[2]. 또한, 2021년 7월 미국 오하이오주 스트롱스빌스에서는 41세 남성을 미성년자 성매매로 수사하는 과정에서 클라우드 스토리지인 Dropbox에 저장된 약 150개의 아동 성 착취 및 포르노 영상이 발견되어 아동 성 착취 및 아동 포르노 소유 등의 혐의로 추가 입건되었다[3].

이에 따라, AccessData, OpenText, BelkSoft, Cellebrite, Elcomsoft. Manet Forensics, Hancom With 등의 주요 디지털 포렌식 도구 개발회사들은 기존 자사 도구에 클라우드 스토리지 데이터 수집 기술을 탑재하거나 클라우드 스토리지 데이터 수집·분석에 특화된 전용 도구를 따로 제공하고 있다. 또한, 클라우드 스토리지 서비스가 본격적으로 상용화되기 시작한 2011년부터 현재까지 Dropbox, Onedrive, Google Drive, Box 등의 다양한 서비스를 대상으로 디지털 포렌식 수사 과정에서 유의미한 데이터 수집·분석에 관한 연구가 꾸준

* 서울과학기술대학교 컴퓨터공학과 (대학원생, sh.seo@seoutech.ac.kr, 대학원생, jek0104@seoutech.ac.kr)
** 서울과학기술대학교 컴퓨터공학과 (교수, chlee@seoutech.ac.kr)

히 진행되어 왔다.

따라서 본 논문에서는 클라우드 스토리지의 정의 및 종류를 살펴보고, 디지털포렌식 관점에서 클라우드 스토리지의 데이터 수집·분석 기술 연구 동향을 분석한다. 또한, 현재 클라우드 스토리지 데이터 수집 기술의 한계 및 향후 연구 방향에 관해 논의한다.

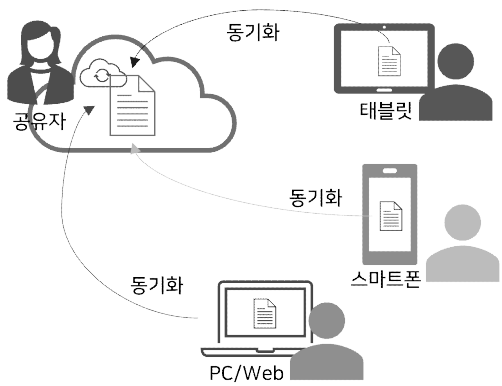
2장에서는 클라우드 스토리지 서비스의 정의하고 분류 기준에 따른 클라우드 스토리지 서비스의 종류와 특특징, 장단점에 관해 설명하고, 3장에서는 클라우드 스토리지에서 데이터 수집 기술과 동향에 대해 설명한다. 또한, 4장에서 현 데이터 수집 기술의 한계와 향후 연구 방향에 관해 논의하고, 5장에서 결론으로 마무리한다.

Ⅱ. 클라우드 스토리지 서비스 개요

본 장에서는 클라우드 스토리지의 개념을 정의하고 장단점에 대해 설명한다. 또한, 서비스 사용 목적과 주체 또는 서비스 방법에 따라 클라우드 스토리지를 분류하고 클라우드 스토리지 종류별 특징과 장단점을 비교분석하여 설명한다.

2.1. 클라우드 스토리지 서비스 정의

클라우드 스토리지는 사용자가 컴퓨터, 스마트폰, 태블릿 등 다양한 기기에서 인터넷망을 통해 데이터를 저장하고 공유하는 형태의 데이터 저장소를 말한다. 이는 데이터 백업뿐 아니라 그림 1과 같이 데이터 공유, 동시작업을 통한 협업 등을 목적으로 사용된다.



〔그림 1〕 클라우드 스토리지의 데이터 공유 및 동시작업

클라우드 스토리지는 컴퓨터, 모바일, 웹 등 다양한 플랫폼에서 장소의 제약 없이 쉽게 접근 가능하고 저장소의 용량 조절이 유연하다는 장점이 있다. 더욱이 저장소의 용량 조절로 인해 발생하는 비용이 적고, 용량 증감 절차가 간단하다. 또한, 침해사고, 자연재해 등으로 인한 스토리지의 물리적 손상으로 인한 데이터 손실, 스토리지 분실 등의 우려가 적다.

하지만 클라우드 스토리지는 공용 인터넷을 통해 저장소에 접근하거나 데이터를 관리함에 따라 데이터 송수신 과정에서 통신 환경에 따른 지연이 발생할 수 있고 스니핑, 스푸핑 등의 여러 보안 위협이 노출될 수 있다.

2.2. 클라우드 스토리지 서비스의 종류

클라우드 스토리지는 서비스 대상에 따라 개인용, 비즈니스용, 클라우드 컴퓨팅용으로 분류할 수 있고 서비스 방식에 따라 퍼블릭, 프라이빗으로 분류할 수 있다.

2.1.1. 서비스 대상에 따른 분류

먼저 클라우드 스토리지는 사용 목적과 주체에 따라 개인용. 비즈니스용, 클라우드 컴퓨팅용으로 구분할 수 있다. 개인용 클라우드 스토리지는 개인의 데이터 백업을 주목적으로 서비스되는 스토리지로 사적인 정보가 주로 저장된다. 특히 모바일 기기에서 사진, 음성, 동영상 등의 미디어 파일이 점차 증가함에 따라 이는 기기와 연동되어 확장된 데이터 저장소로 활용되고 있다. 또한, 개인의 모바일 기기 교체 주기가 단축됨에 따라 편리를 위해 연락처, 메일, 문자메시지, 메신저 대화 기록, 인터넷 검색 기록, 애플리케이션 설정 등의 개인적인 모바일 데이터 백업이 개인용 클라우드 스토리지에 저장될 수 있다.

비즈니스용 클라우드 스토리지는 회사, 기업, 학교 등의 단체를 대상으로 서비스되는 스토리지로 데이터 공유, 공동작업, 데이터 축적 및 백업을 목적으로 사용된다. 이에 따라 해당 클라우드 스토리지 내에는 단체 운영을 위한 데이터, 업무 관련 정보, 고객 정보, 마케팅 정보, 구성원의 개인정보 등이 저장될 수 있다. 또한, 비즈니스용 클라우드 스토리지는 스토리지를 설정·관리하는 관리자 계정과 관리자 계정이 할당한 사

용자 계정으로 구성된 그룹 형태로 관리된다. 이때 관리자는 비즈니스 그룹의 스토리지 용량, 사용자 계정 할당, 스토리지 내 데이터의 접근 권한, 사용자 인증방식 설정 등을 관리한다.

클라우드 컴퓨팅용 클라우드 스토리지는 클라우드 컴퓨팅 플랫폼에서 웹앱, Enterprise Resource Planning(ERP), Customer Relationship Management (CRM), 그룹웨어 등 비즈니스 애플리케이션 실행을 위해 사용된다. 이는 저장되는 데이터의 종류에 따라 객체 스토리지, 파일 스토리지, 블록 스토리지, 아카이브 스토리지 등으로 구분할 수 있고 데이터 블록, 객체, 파일, 컴퓨팅 엔진, 소스코드, 학습 데이터 셋, 백업 등이 저장된다[4][5]. 비즈니스 앱의 용도와 목적에 따라 사용되는 클라우드 컴퓨팅용 클라우드 스토리지의 종류와 저장되는 데이터, 데이터의 저장 형태가 상이하다.

〔표 1〕 서비스 대상에 따른 클라우드 스토리지 분류별 특징

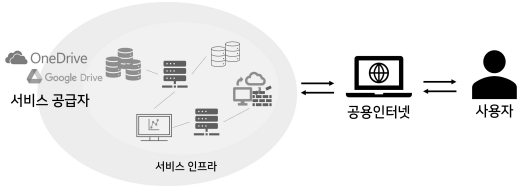
	특징
개인용	✓ 개인의 데이터 백업을 주목적으로 사용 ✓ 모바일 기기에서 로컬 스토리지와 자동 동기화 기능 제공 ✓ 연락처, 메일, 문자메시지, 메신저 대화 및 인터넷 검색 기록, 미디어 파일 등의 모바일 백업 데이터, 개인정보 등이 저장될 수 있음 ✓ Onedrive, Google Drive, Dropbox, Amazon Drive, iCloud, Mega Cloud, pCloud, 네이버 Mybox 등
비즈니스용	✓ 회사, 기업, 학교 등 단체의 데이터 공유, 공동작업, 협업, 데이터 백업 등을 목적으로 사용 ✓ 관리자와 사용자 계정으로 구성된 그룹 형태로 관리 ✓ 회사의 업무 관련 데이터, 고객 정보 ✓ Google Workplace, Onedrive Business Plan 1, 2, Dropbox Business Standard, Advanced 등
클라우드 컴퓨팅용	✓ 클라우드 컴퓨팅 플랫폼에서 비즈니스 앱 실행을 위해 사용 ✓ 스토리지 용량, 데이터 송수신/입출력 횟수별 가격 책정 ✓ 비즈니스 앱 종류에 따라 스토리지 종류와 데이터 저장 형태, 저장되는 데이터의 종류가 상이함 ✓ AWS Storage (S3, EFS, FSx, EBS, Data Sync 등), Azure Storage (Disk Storage, Blob Storage, Data Lake, NetApp File 등), Naver Cloud platform Storage (Object Storage, Archive Storage, Block Storage, Backup, NAS 등)

클라우드 스토리지의 사용 목적과 주체에 따른 클라우드 스토리지 종류별 특징은 표 1과 같다.

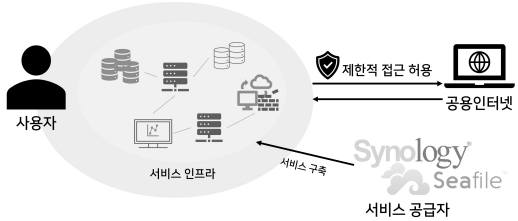
2.1.2. 서비스 방식에 따른 분류

클라우드 스토리지는 서비스 방식에 따라 퍼블릭 클라우드 스토리지와 프라이빗 클라우드 스토리지로 구분할 수 있다. 퍼블릭 클라우드 스토리지는 그림 3과 같이 스토리지 서비스 인프라가 사용자와 분리되어 서비스 공급자에 의해 관리되고 사용자는 공용 인터넷을 통해 공급받은 개별 스토리지를 사용하는 형태의 클라우드 스토리지를 말한다. 이는 서비스 공급자가 시스템의 모든 관리, 유지보수를 담당하므로 사용자가 전문적인 지식이 없어도 웹, 애플리케이션, API 등을 이용해 쉽게 저장소를 이용 및 관리할 수 있다. 하지만 데이터 접근 권한, 인증 및 보안 기술이 전적으로 서비스 공급자에 의해 관리되고 사용자에게 제공되는 설정 범위에 따라 데이터 관리가 제약적일 수 있다.

Google, Microsoft 등의 글로벌 기업에서 제공하는 주요 퍼블릭 클라우드 스토리지는 데이터 서버가 여러 국가에 분산되어 있으므로 사용자의 스토리지 내 파일이 여러 지역에 걸쳐 저장될 수 있고 사용자가 실제 데이터의 저장 위치를 확인하기 어렵다. 이에 따라 수사관이 클라우드 스토리지 내 데이터를 수집하기 위해



〔그림 2〕 퍼블릭 클라우드 스토리지



〔그림 3〕 프라이빗 클라우드 스토리지의

서는 클라우드 스토리지 서비스를 직접 이용하거나 서비스 공급자의 협조가 필요하다. 현재 상용 중인 퍼블릭 클라우드 스토리지 서비스는 대표적으로 Microsoft의 Onedrive, Google의 Google Drive, 네이버의 Mybox, Amazon의 Amazon Drive, Dropbox, Megacloud 등이 있다.

프라이빗 클라우드 스토리지는 그림 2와 같이 스토리지 서비스 인프라를 사용자가 소유하고 있고 단일 조직 또는 단일 사용자에 의해서만 사용되는 스토리지를 말한다[6]. 이는 인프라를 소유하는 사용자에 의해 시스템이 유지·관리되기 때문에, 데이터 제어에 제약이 없고 높은 수준의 보안 기능을 적용할 수 있다. 이때 관련 Synology, Seafile 등의 서비스 공급자는 사용자의 클라우드 스토리지 서비스 인프라 구축에만 관여한다. 따라서 사용자는 클라우드 스토리지 서비스를 이용·관리하기 위한 전문적인 지식이 요구될 수 있다. 또한, 프라이빗 클라우드 스토리지는 서비스 인프라를 사용자가 소유하기 때문에 데이터 서버 접근이 용이하고 퍼블릭 클라우드 스토리지에 달리 데이터 서버에서 대상 데이터에 대해 물리적으로 bit-by-bit 이미징이 가능하다. 현재 상용 중인 프라이빗 클라우드 스토리지 서비스로는 Synology, Seafile Seagate, HPE 등이 있다.

Ⅲ. 클라우드 스토리지 포렌식 분석 연구 동향

현재까지 클라우드 스토리지에 대한 디지털포렌식 관점의 분석 연구는 클라우드 스토리지가 본격적으로 상용화되기 시작한 2011년부터 꾸준히 진행되어왔다. PC, 모바일 플랫폼에서 Windows, MacOS, Ubuntu, Android, iOS 등 다양한 OS를 환경으로 아티팩트 수집 및 분석 연구가 수행되었다. 또한, Chrome, Firefox, Internet Explore 등의 웹에서 클라우드 스토리지를 실행했을 때 수집할 수 있는 아티팩트에 관한 연구도 수행되었다. 분석 환경별로 아티팩트 분석 연구가 수행된 클라우드 서비스를 정리하면 표 2와 같다.

〔표 2〕 아티팩트 분석 연구가 수행된 클라우드 서비스의 분석 환경에 따른 분류표

분석 환경		분석 대상 클라우드 서비스
PC	Windows	Google Cloud[7][19][22],Dropbox[8][9][13][11][12][22], Evernote[8][12], ucloud[8], N Drive[8], Daum Cloud[8], Skydrive[9], Skydrive[9], Box[14], iCloud[21, Mega[21], Box[21], Amazon Cloud Drive[21][22], ADrive[20], pCloud[16], CloudMe[10], Amazon Cloud Drive[15], hubiC[18], Amazon S3[12], Google Docs[12]
	MacOS	CloudMe[10], hubiC[18], Dropbox[12], Amazon S3[12], Google Docs[12], Evernote[12]
	Ubuntu	CloudMe[10]
Mobile	Android	Dropbox[8][11][12][17], Evernote[8][12], ucloud[8], N Drive[8], Daum Cloud[8], pCloud[16], Amazon S3[12], Google Docs[12], Box[11], SugarSync[11]
	iOS	Dropbox[8][11][12][16], ucloud[8], N Drive[8], Daum Cloud[8], hubiC[18], Amazon S3[12], Google Docs[12], Evernote[8][12], Box[11], SugarSync[11]
Web	Chrome	Dropbox[11], AWS EC2[15], Amazon S3[15], Rackspace[15], Ucloud[15], Tcloud[15], Azure[15], ThinkFree[15], Zoho Office[15], MS Live Online[15], Google Docs[15, Glice OS[15], Photoshop Express Online[15], ADrive[20], iCloud[21], Mega[21], Box[21], Amazon Cloud Drive[21], Onedrive[21], hubiC[18]

3.1. 모바일 클라우드 스토리지 아티팩트 분석 연구

김동호[7]는 스마트폰 사용자의 구글 계정에 저장되어있는 데이터들의 종류와 구조를 분석하고 디지털포렌식 수사 과정에서 활용 가치가 높은 항목들을 선별하여 정리하였다. 또한, 선별된 항목의 데이터를 수사 업무에 효과적으로 활용하는 방안을 제시하고, Google 클라우드 데이터가 사건 해결을 위해 중요한 단서가 될 수 있는지를 활용 사례를 제시함으로써 증명하였다.

정현지 외 2명[8]은 iOS, 안드로이드 운영체제를 대상으로 Dropbox, Evernote, ucloud, N드라이브, 다음 클라우드의 5개 클라우드 스토리지 서비스의 아티팩트를 수집하는 방법론을 제시하고 수집 데이터를 분석하여 디지털 포렌식 관점에서 유의미한 아티팩트를 정리하였다.

Teing, Yee-Yang 외 5명[9]은 Android 4.4.4, iOS 7.1.2 환경에서 프라이빗 클라우드 스토리지인 Seafile에 대한 포렌식 분석을 수행하였다. 또한, 퍼블릭 클라우드 스토리지와 다른 프라이빗 클라우드 스토리지의 특성을 고려하여 프라이빗 클라우드 스토리지 수사 프레임워크를 제안하였다. 분석 결과, 모바일 기기에서 파일 동기화 정보, 인증 정보, 파일 암호화 관련 정보, 파일 업·다운로드 기록 등의 데이터를 수집할 수 있음을 확인하였다.

Teing, Yee-Yang 외 2명[10]은 iOS 7.1.2, Android 4.4.4 환경에서 CloudMe 클라우드 스토리지에 대한 아티팩트 분석을 수행하였다. 분석 결과, db.sdb, cache.db 등의 데이터베이스 파일에 클라우드 스토리지 내 파일을 열람한 기록이 남는 것을 확인하였고, 클라우드 스토리지 사용과 관련한 로그파일, 웹 캐시 등이 앱 내부 저장소에 저장되는 것을 확인하였다.

Grispos, George 외 2명[11]은 iOS 3.0, Android 2.1, Android 2.3 환경에서 Dropbox, Box, Syncplicity, SugarSync의 클라우드 스토리지 4종에 대한 아티팩트 분석 연구를 수행하였다. Celebrite 사의 UFED를 이용하여 스마트폰 데이터를 수집 및 분석하였으며, 분석 결과 클라우드 스토리지에 저장된 이미지 파일, 데이터 송수신 로그(transaction log), 동기화 및 설정과 관련한 각종 json, xml 파일 등이 스마트폰 내 저장되는 것을 확인하였다.

Chung, Hyunji 외 3명[12]은 Android, iOS 환경에서 클라우드 스토리지 Amazon S3, Dropbox의 아티팩트를 분석하였다. 분석 결과, 애플리케이션의 내부 저장소에 저장되는 데이터베이스, xml, plist 등의 파일에서 사용자 ID/PW, 파일 업·다운로드 리스트, 데이터 접근 시간, 마지막 동기화 시간, 파일 수정 시간, 파일 이름, 파일 유형 등의 아티팩트를 확인하였다.

3.2. PC 클라우드 스토리지 아티팩트 분석 연구

남기욱 외 3명[13]은 Windows 환경에서 Dropbox 클라우드 아티팩트를 수집하고 분석하는 연구를 수행하였다. 기존 Dropbox 관련 연구에서 아티팩트로 제시된 파일 로드 및 동기화 관련 파일(filecache.dbx, config.dbx 등)이 삭제되거나 복호화 방안이 달라진 것을 확인하고, Dropbox에서 추출할 수 있는 새로운 아티팩트를 분석하여 제시함으로써 극복하는 방안을 마련하였다. 또한, NTFS 시간 변화를 통해 로드 및 동기화에 대한 행위를 구분함으로써 분석을 통해 제시한 아티팩트에서 시간 정보 수집의 한계도 극복하였다.

윤혜민 외 4명[14]은 Windows 10 환경에서 Box 클라우드에 대한 포렌식 분석을 수행하였다. VMware에 Windows 10 x64를 설치하고, Box 클라우드에서 수행할 수 있는 사용자 행위인 설치, 계정 생성, 로그인, 업로드, 다운로드, 동기화, 삭제 및 복원, 프로그램 삭제 등에 대한 시스템 내 흔적 데이터를 분석하였다. 분석을 위한 사용자의 행위를 수행한 후, VMware snap shot 기능으로 상태를 저장하고, .vmdk 파일을 .vhd 파일로 변환하여 Autopsy를 활용해 수집한 아티팩트를 이용해 분석을 수행하였다.

정일훈 외 3명[15]은 IaaS(Infra as a Service)에 대한 디지털 포렌식 관점의 조사방법과 IaaS 모델 중 Amazon Web Service(AWS)와 Rackspace에 대해 데이터 수집 및 분석 방안에 대해 제시하였다. 클라이언트 PC에서 해당 서비스의 사용 흔적 확인, 서비스의 흔적 데이터 수집 및 분석, 로그인 정보 획득과 서비스 접속을 통한 관련 데이터 확인하는 방법들을 통해 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 조사 방법을 구체화 하였다.

Ahmad, Nur Hayati 외 3명[16]은 Windows 7 환경에서 pCloud 클라우드 스토리지에서 디지털 포렌식 데이터 수집 및 아티팩트 분석 연구를 수행하였다. Virtual Box를 이용하여 가상 환경을 구성하고 파일 업로드, 파일 다운로드, 로그인 등의 사용자 행위를 수행 후 메모리를 수집하여 HxD를 이용하여 바이너리 상태의 메모리를 분석하였다. 분석 결과 사용자 행위별로 사용자의 크리덴셜(ID/PW), 업·다운로드 파일, 시간 정보를 메모리에서 수집할 수 있음을 확인하였다.

Lim, Shu Yun, 외 3명[17]은 Windows 10 환경에

서 Dropbox 클라우드 스토리지를 분석하였다. 파일 시스템, 네트워크, 메모리에서 데이터를 수집하고 레지스트리, 휴지통, 이벤트 로그, 네트워크 패킷, 메모리 캡처 등을 분석하여 Dropbox의 사용 흔적을 확인하였다. 분석 결과로 Dropbox의 인증 host_id, Host_id와 관련한 config.db 등을 확인하였다.

Teing, Yee-Yang 외 2명[10]은 Windows 8.1, Ubuntu 14.04.1, Mac OS X Mavericks에서 CloudMe 클라우드 스토리지에 대한 아티팩트 분석을 수행하였다. 파일 시스템, 레지스트리, 메모리 관점에서 포렌식 분석을 수행하였으며, 그 결과 CloudMe 사용 로그가 담긴 데이터베이스 파일(cache.db), 동기화 설정 정보가 담긴 Sync.conf, clientID를 기록하는 레지스트리 경로 등을 확인하였다.

Blakeley, Ben 외 3명[18]은 Windows 8.1 환경에서 클라우드 스토리지 hubiC의 아티팩트 분석을 수행하였다. 가상 머신을 이용하여 파일 시스템, 메모리, 네트워크의 데이터를 분석하였으며, 그 결과 데이터 열람 기록, 이미지 파일, 접속 기록, 사용자 크리덴셜, 동기화 기록, 설치 기록 등의 아티팩트를 확인하였다.

3.3. Web 클라우드 스토리지 아티팩트 분석 연구

김도현 외 2명[19]은 디지털 포렌식 관점에서의 구글 클라우드 데이터를 통해 사용자 행위를 분석하는 연구를 수행하였다. 구글 Takeout에는 약 28개의 구글 서비스의 데이터를 포함하고 있으며, 이 중 약 11개가 디지털포렌식 관점에서 사용자 행위 분석에 유용하게 사용할만한 정보를 포함하고 있다. 따라서 이 서비스에 대한 데이터에 대하여 타임 라인, 검색 및 웹브라우징 내역, 파일 정보, 위치 정보 분석 등 4가지 관점에서 분석하고, 각 관점으로 분석한 내용을 통합적으로 활용하여 사용자 행위를 분석하는 방안을 제시하였다. 또한, 구글 Takeout의 데이터 분석을 지원하는 도구를 개발하고 오픈 소스를 공개하였다.

Rochmadi, Tri 외 1명[20]은 윈도우 환경에서 라이브 포렌식 관점으로 활성 데이터들을 분석하고 메모리, 파일 시스템에 Adrive 실행 관련 데이터가 남는 것을 확인하였다. 메모리에서 드라이브 실행과 관련한 url, 로컬 저장소 경로에 파일명 및 파일 스템프, 브라우저 히스토리에서 프로그램 설치 내역이 남는 것을 확인하였다.

Easwaramoorthy, Sathishkumar 외 4명[21]은 Firefox, Internet Explorer, Google Chrome 브라우저에서 One Drive, Amazon Cloud Drive에 대한 포렌식 데이터 분석 연구를 수행하였다. Windows 7 환경에서 각 브라우저들을 이용해 클라우드 스토리지를 실행하고 관련 데이터를 분석하였으며, 분석결과 Cache, Cookie, Histroy 등에 클라우드 스토리지와 관련한 데이터가 저장되는 것을 확인하였다.

Ⅳ. 클라우드 스토리지 데이터수집의 한계

클라우드 스토리지 서비스 회사에서 제공하는 데이터 저장 용량은 최소 2GB에서 최대 10TB로 TB 단위까지 확대되었다. 따라서, 클라우드 스토리지 내 모든 데이터를 수집한 후 분석하는 것은 최대한 적은 시간 내에 증거를 분석해야 하는 디지털포렌식 수사 환경을 고려할 때 한계가 있다. 또한, 사건과 연관이 없는 데이터를 포함한 모든 데이터를 클라우드 스토리지에서 수집하는 것은 프라이버시 문제가 발생할 수 있다.

최근 이러한 한계를 극복하기 위해 클라우드 스토리지 데이터에 원격으로 접근할 수 있는 OpenAPI를 활용한 데이터 선별 수집 방안에 관한 연구가 수행되었다.한중수 외 5명[22]은 클라우드 저장소 서비스 내의 파일들에 대해서도 기존 로컬 저장소 파일들과 마찬가지로 선별 수집하는 방법에 대한 연구를 수행하였다. OAuth2.0 프로토콜을 기반으로 동작하는 OpenAPI를 활용하여 사용자의 클라우드 스토리지 데이터 접근 방안에 대해 정리하고 이를 활용한 데이터 선별 수집 방법을 제안하였다. 사용자의 ID/PW가 확보되었다고 가정할 때, OpenAPI를 이용하여 클라우드 스토리지 내 저장된 파일들의 메타데이터를 먼저 수집하고, 사건과 관련 있는 파일 정보만 선별하여 파일을 서버에 요청함으로써 원격으로 파일을 선별 수집하는 방안을 제시하였다.

하지만 OpenAPI를 활용하여 클라우드 스토리지의 데이터를 수집하기 위해서는 접근하고자 하는 스토리지 소유자의 ID와 PW가 필요하다는 한계가 있다.

Ⅴ. 결 론

본 논문에서는 클라우드 스토리지의 개념을 설명하고 서비스 대상, 서비스 방식의 분류 기준에 따른 클라

우드 스토리지 종류별 특징과 장단점을 비교분석하였다. 또한, 클라우드 스토리지 서비스에 대한 디지털포렌식 관점의 아티팩트 수집 및 분석 연구 동향을 살펴보고, 클라우드 스토리지 데이터 수집의 한계를 기술하였다.

스토리지 용량의 증가와 프라이버시 이슈로 인해 발생하는 클라우드 스토리지 데이터 수집의 한계를 극복하기 위해 OpenAPI를 이용하여 원격으로 데이터를 선별 수집하는 방안이 제안되었으나, OpenAPI를 활용하기 위해서는 소유자의 계정 정보(ID/PW)가 필요하다는 한계가 있다.

따라서, 소유자의 계정정보를 제공받을 수 없는 상황에서도 PC, 모바일 등에서 수집한 아티팩트를 활용하여 데이터를 원격 수집하는 방안에 관한 연구가 수행될 필요가 있다.

참 고 문 헌

[1] 고세란, “클라우드 서비스 이용 추이 및 현황”, ・KISIDI STAT Report Vol.21-12, pp.1-8, 2021

[2] Daniel Ball, “Northeast Ohio Priest Pleads Guilty to Charges of Sex Trafficking of a Minor, Sexual Exploitation of a child and Possenssion of Child Pornography”, United States Depoartment of Justice, 2021.07.16, URL:https://www.justice.gov/usao-ndoh/pr/northeast-ohio-priest-pleads-guilty-charges-sex-trafficking-minor-sexual-exploitation, Accessed : 2022.04.15.

[3] SBS News, ““모를 줄 알았지?” 클라우드에 불법 촬영 영상 숨긴 20대 덜미“, 2019.09.10., URL:https://news.sbs.co.kr/news/endPage.do?news_id=N1005432671, Accessed : 2022.04.15.

[4] Amazon Web Service, “AWS 기반 클라우드 스토리지”, 2021.11.24., URL:https://aws.amazon.com/ko/products/storage/, Accessed : 2022.04.15.

[5] Google, Cloud, “Cloud Storage 옵션“, 2021.11.24., URL:https://cloud.google.com/products/storage, Accessed : 2022.04.15.

[6] NIST, “The NIST definition of Cloud Computing, Peter Mell and Timothy Grance”, 2011, URL:https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, Accessed : 2022.04.15.

[7] Ahmad, N. H., Hamid, A. S. S. A., Shahidan, N. S. S., Ariffin, K. A. Z., ”Cloud Forensic Analysis on pCloud: From Volatile Memory Perspectives.” In International Conference for Emerging Technologies in Computing, pp. 3-15, Springer, Cham, August 2020

[8] 정현지, 박정흠, 이상진 "클라우드 스토리지 서비스에 대한 디지털 포렌식 조사 방법" 디지털포렌식연구 , (8), pp.1-26, 2011

[9] Chung, H., Park, J., Lee, S., & Kang, C, “Digital forensic investigation of cloud storage services.” Digital investigation, 9(2), pp.81-95, 2012

[10] Grispos, G., Glisson, W. B., Storer, T. , “Recovering residual forensic data from smartphone interactions with cloud storage providers”. arXiv preprint arXiv:1506.02268, 2015

[11] 남기욱, 김동현, 최지성, 이상진, “Windows 환경에서 드롭박스(Dropbox) 애플리케이션 흔적 조사.”, 디지털포렌식연구, 14(1), pp.45-58, 2020

[12] Teing, Y. Y., Homayoun, S., Dehghantanha, A., Choo, K. K. R., Parizi, R. M., Hammoudeh, M., Epiphaniou, G. “Private cloud storage forensics: Seafile as a case study.”, In Handbook of Big Data and IoT Security, Springer, Cham, pp. 73-127, 2019

[13] 윤혜민, 김재욱, 황은비, 김해니, 권태경, “Windows 10 환경의 Box 클라우드 아티팩트 분석.”, 정보보호학회지, 29(6), pp.29-37, 2019

[14] 김도현, 김준기, 이상진, “디지털 포렌식 관점에서의 구글 클라우드 데이터 분석 연구.” 한국정보통신학회 종합학술대회 논문집, 24(1), pp.102-104, 2020

[15] 김동호. "구글 클라우드 데이터의 수사활용 방안에 관한 연구." 국내석사학위논문 고려대학교, 2019.

[16] Blakeley, B., Cooney, C., Dehghantanha, A., & Aspin, R., “Cloud storage forensic: hubiC as a case-study.”, IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 536-541, November 2015

[17] Teing, Y. Y., Dehghantanha, A., Choo, K. K. R., “CloudMe forensics: A case of big data forensic investigation.” Concurrency and Computation:

Practice and Experience, 30(5), e4277, 2018
[18] 정일훈, 오정훈, 박정흠, 이상진, “IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구.” 정보보호학회논문지, 21(6), pp.55-65, 2011
[19] 한중수, 이승용, 오정훈, 김준수, 정혜진, 황현욱, “클라우드 스토리지 서비스에 대한 메타데이터 기반 파일선별 수집 방법 및 구현.”, 디지털포렌식연구, 14(3), pp.305-315, 2020
[20] Rochmadi, Tri, Dadang Heksaputra, "Forensic analysis in cloud storage with live forensics in windows (adrive case study).", Int. J. Cyber-Secur, Digit. Forensics, 8.4 , pp.292-297, 2019
[21] Ko, Aye Chan, Wint Thida Zaw, "Digital forensic investigation of Dropbox cloud storage service.", Network Security and Communication Engineering (Ed: Kennis Chan), CRC Press: İngiltere, pp.147-150, 2015
[22] Easwaramoorthy, S., Thamburasa, S., Samy, G., Bhushan, S. B., Aravind, K. (2016, April). Digital forensic evidence collection of cloud storage data for investigation,” In 2016 International Conference on Recent Trends in Information Technology (ICRTIT), pp. 1-6, Apri 2016

〈저 자 소 개〉

서 승 희 (Seunghee Seo)
학생회원
2017년 2월 : 서울과학기술대학교 컴퓨터공학과 학사
2019년 2월 : 서울과학기술대학교 컴퓨터공학과 석사 (디지털 포렌식 전공)
2020년 3월~현재 : 서울과학기술대학교 컴퓨터공학 박사과정 (디지털 포렌식)
<관심분야> 디지털포렌식, 사이버보안, 블록체인, 암호

김 주 은 (Jueun Kim)
학생회원
2022년 2월 : 동의대학교 컴퓨터공학과 졸업
2022년 3월~현재 : 서울과학기술대학교 컴퓨터공학과 석사과정
<관심분야> 디지털포렌식, 사이버보안

이 창 훈 (Changhoon Lee)
종신회원
2001년 2월 : 한양대학교 자연과학부 수학전공 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2008년 2월 : 고려대학교 정보경영전문대학원 정보보호전공 박사
2008년 4월~2008년 12월 : 고려대학교 정보보호연구원 연구교수
2009년 3월~2012년 2월 : 한신대학교 컴퓨터공학부 조교수
2012년 3월~2015년 3월 : 서울과학기술대학교 컴퓨터공학과 조교수
2015년 4월~현재 : 서울과학기술대학교 컴퓨터공학과 부교수
2020년 4월~현재 : 서울과학기술대학교 컴퓨터공학과 교수
<관심분야> 암호, 디지털포렌식, 사이버보안