클라우드 환경에 적합한 디지털 포렌식 수사 모델

이 규 민* · 이 영 숙**

요 약

클라우드 컴퓨팅은 인터넷이 가능한 환경에서 다양한 단말을 통해 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 이용할 수 있는 서비스이다. 편리성과 효율성, 비용 절감의 이유로 최근 이용률이 급증하였다. 하지만 정보의 집중화로 인해 범죄의 표적이 되거나 클라우드 서비스를 악용하는 범죄가 발생하였다. 기존 디지털 포렌식 절차는 개인 단말기를 대상으로 하는 수사에 적합하다. 본 논문은 기존 디지털 포렌식 수사 절차로 클라우드 환경을 조사할 경우 발생하는 취약점들을 분석하여 새로운 수사 모델을 제안하였다. 제안된 수사 모델은 계정정보를 획득할 수 있는 방법을 추가하였으며, 공공 클라우드와 사설 클라우드를 아울러 적용할 수 있다. 또한, 클라우드 서비스는 쉽게 접근이 가능하여 디지털 증거 인멸 가능성이 높기에 계정 접근 차단 단계를 추가함으로써 수사 모델을 보강하였다.

Digital Forensic Model Suitable for Cloud Environment

Gymin Lee* · Youngsook Lee**

ABSTRACT

Cloud computing is a service that to use IT resources (software, storage, server, network) through various equipment in an Internet-enabled environment. Due to convenience, efficiency, and cost reduction, the utilization rate has increased recently. However, Cloud providers have become targets for attack Also, Abuse of cloud service is considered as the top security threat. The existing digital forensic procedures are suitable for investigations on individual terminals. In this paper, we propose a new investigation model by analyzing the vulnerable points that occur when you investigate the cloud environment with the existing digital forensic investigation procedure. The proposed investigation model adds a way to obtain account information, and can apply public cloud and private cloud together. Cloud services are also easily accessible and are likely to destroy digital evidence. Therefore, the investigation model was reinforced by adding an account access blocking step.

Key words : Digital Forensic, Cloud Computing, Cloud Service, Digital Evidence, Procedure of Investigation

접수일(2017년 9월 5일), 수정일(1차: 2017년 9월 27일),
게재확정일(2017년 9월 30일)

* 호원대학교 사이버수사경찰학부
** 호원대학교 사이버수사경찰학부(교신저자)

1. 서 론

클라우드 서비스는 사용자 단말에 특정 소프트웨어를 설치하지 않아도 인터넷 접속이 가능하면 언제 어디서나 이용 가능하다[1]. 클라우드 서비스가 대두되기 시작하면서 다양한 연령대가 서비스를 사용하고 있으며, 이용 현황은 점점 증가하고 있는 추세이다[2]. 또한, 업무의 효율성, 시스템 관리 비용 절감 등의 이유로 많은 기업 및 정부 기관에서도 클라우드 서비스를 도입하고 있다[3].

서비스 이용률의 급증으로 클라우드 서비스가 범죄의 수단으로 이용되거나 표적이 되는 현상이 나타나고 있다[4]. 많은 사람의 개인정보 및 다양한 정보가 저장되어 있어 보안사고 발생 시 그 피해 규모가 상당하다. 기존 압수수색 절차는 개인 단말 또는 저용량 서버에 적합하다. 하지만 데이터의 저장 공간이 개인 단말에서 중앙 집중화된 서버로 변화되고 있는 시점에 기존 수사 절차를 클라우드 환경에 적용하였을 경우 많은 문제점이 속출한다. 따라서 기존 디지털 증거의 압수수색 절차에 변화가 필요하여 본 논문은 클라우드 환경에서 디지털 증거의 압수수색 시 발생하는 취약점 분석을 통해 새로운 수사 모델을 제시하도록 한다.

2. 클라우드 컴퓨팅 서비스의 개념과 현황

2.1 클라우드 컴퓨팅 서비스의 현황

일반적으로 클라우드 컴퓨팅의 정의가 가장 많이 인용되고 있는 기관은 NIST(National Institute of Standard and Technology, 미국국립표준연구소)이다. 하지만 클라우드 컴퓨팅에 대한 정의는 각 학계 및 기관마다 다르게 표현되고 있다. 이를 정리하면 클라우드 컴퓨팅은 '이용자의 요구에 따라 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 공급하고 그에 따른 비용을 지불하는 서비스'라고 정의할 수 있다[1].

인터넷 사용의 증가에 따라 클라우드 서비스를 이용하는 사람들도 매년 증가하고 있다. 한국인터넷진흥원이 2015년도에 실시한 인터넷 이용 실태 조사에 따르면 만 3세 이상 인구의 85.1%인 41,940천명이고 만 12세 이상 인터넷 이용자 중 23.7%가 클라우드 서비스 이용자로 나타났다[2]. 개인뿐만 아니라 공공기관 및 기업에서의 이용도 증가하였다. 미래창조과학부와 행정자치부 주관으로 클라우드 수요조사가 실시되었으며, 그 결과는 <표1>과 같다[3].

<표 1> 클라우드 이용 현황 및 이용 계획

구 분	~ 2016년			2017년			2018년		
종류*	G	자체	민간	G	자체	민간	G	자체	민간
기관수	20	84	23	17	49	51	29	57	59
	127			117			145		

G: 정부통합전산센터 클라우드 / 자체 : 기관 구축·이용 / 민간 : 상용클라우드

정부는 지난 2016년은 클라우드컴퓨팅법 시행 후 첫해인 만큼 클라우드 산업육성을 위해 제도적 기반 조성에 주력해 왔으며, 2017년에는 클라우드가 본격 확산이 될 수 있도록 총력을 기울일 계획이라고 밝혔다.

클라우드 환경에서 발생하는 범죄들을 분류하였을 때 신종범죄와 내용범죄, 재산범죄로 구분할 수 있다. 해킹 및 보안침해는 서비스 제공자의 보안강화와 비례하게 진화되고 있으므로 기존 사이버범죄와 동일하게 신종범죄로 분류된다. 불법정보 은닉 및 유출은 그 내용에 따라 분류될 수 있으므로 내용범죄에 속하며, 명예훼손, 비방, 음란물 등이 포함될 수 있다. 재산상의 피해를 보았을 경우 성립되는 재산범죄에는 해킹 및 보안침해, 개인정보침해, 저작권 침해 등이 존재한다. 이런 유형의 범죄는 서비스 제공자와 이용자 그리고 제 3자까지 피해자가 될 수 있다. <표 2>에서는 신종범죄와 내용범죄, 재산범죄로 분류될 수 있는 범죄 유형을 정리하였다[4].

<표 2> 범죄유형별 분류

구 분	범죄 유형
신종범죄	해킹 및 보안침해
내용범죄	불법정보 은닉 및 유출
이용상의 재산범죄	해킹 및 보안침해, 개인정보침해, 저작권침해

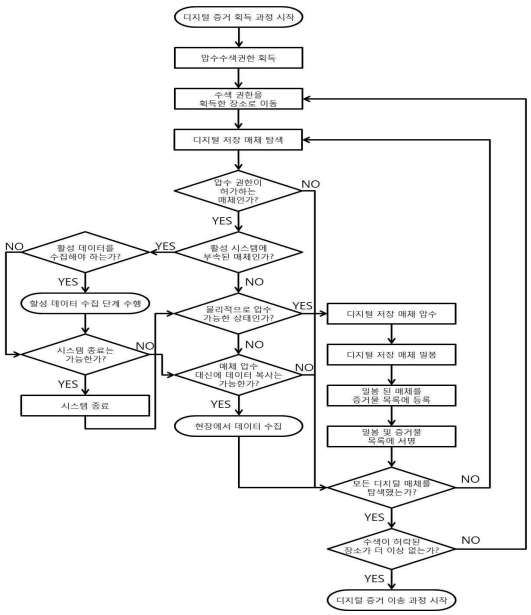
2.2 클라우드 서비스 관련 국내 법제 현황

해외에서는 기업들이 발 빠르게 클라우드 서비스 시장을 선점하고 원천 기술을 보유할 수 있도록 다양한 정책 마련과 지원을 해주고 있다. 반면 우리나라의 클라우드 산업은 글로벌 수준에 비해 많이 부진한 상황이다. 세계적으로 클라우드로 서비스가 전환되고 있는 만큼 우리나라도 안정적으로 서비스를 제공하기 위해 법 제도적으로 뒷받침이 필요했다. 그래서 약 3년 동안의 입법과정을 걸쳐 2015년 9월 27일에 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률(이하 클라우드컴퓨팅법 이라 한다)을 제정하였다. 이 법률은 이용자 보호를 위한 방안 마련과 클라우드 서비스를 안전하게 사용할 수 있는 환경을 조성할 목적으로 마련되었으며, 2015년 9월 28일부터 시행되었다[5].

3. 클라우드 환경에 적합한 디지털 포렌식

3.1 기존 디지털 포렌식 수사

디지털 포렌식의 주목적은 디지털 증거를 사법기관에 제출하는 과정에서 법정 유효성을 확보하는 것이다. 디지털 정보는 위·변조가 용이하고 훼손될 가능성도 크다. 따라서 처리 과정에서 실수를 최소화하기 위해서 경찰청은 디지털 증거를 처리하는 일련의 과정을 규정한 '디지털 증거처리 표준 가이드라인'을 만들었다. (그림 1)은 디지털 증거 획득 과정을 표준화한 것이다. 디지털 증거처리 표준 가이드라인에는 (그림 1) 이외에 기업부정, 살인 및 자살, 저작권 침해 등 사건 유형별로 포렌식 수사 절차를 규정해 놓았다[6].



(그림 1) 디지털 증거 획득 과정

3.2 클라우드 환경에서 디지털 증거 압수수색 과정의 취약점

3.2.1 압수수색 대상과 범위 불명확

디지털 증거를 압수수색하는 과정은 영장주의에 의하여 진행된다. 영장주의란 체포, 구속, 압수수색과 같은 수사행위를 할 때 사람의 신체 및 의사의 자유에 제한을 가하는 것이다[7]. 법관이 발부한 압수수색영장에는 현행 형사소송법 제114조에 따라 압수할 물건 및 수색할 장소를 명시하게 되어 있다. 이에 해당하지 않는 범위에서 수집된 증거라면 그 증거능력이 부정될 수 있다. 하지만 디지털 증거를 압수수색하는 절차에서 가장 문제 되는 것이 압수수색 대상과 범위를 정하는 것이다. 전자적 정보가 가지고 있는 특성 중 비가시성·비가독성 등에 의해 해당 디지털 자료를 열어 보지 않고는 범죄와의 연관성을 찾기 힘들며, 네트워크를 통해서 전송 및 저장이 가능하기 때문에 압수

수색 대상과 범위를 특정 하는 것은 어려울 수밖에 없다. 하지만 이러한 어려움 때문에 영장주의의 적용이 배제되거나 완화되지는 않는다[8].

3.2.2 과잉압수수색과 개인정보침해

클라우드 스토리지 서버는 세계 각지에 물리적으로 분산되어 관리된다. 따라서 하나의 스토리지에는 많은 이용자의 정보도 함께 저장되어 있을 수 있다. 포괄적으로 클라우드 스토리지 서버의 자료를 압수수색하여 분석할 경우 피압수자에게 개인정보침해와 과잉압수수색을 진행했다는 비판을 받을 수 있다[8].

3.2.3 동시 접속 문제

용의자가 클라우드 컴퓨팅 환경에 저장된 증거를 은닉하거나 삭제·위조·변조를 할 수 없는 상황에 처했을 경우 공범에 의해 이를 쉽게 행할 수 있다. 계정정보와 함께 인터넷이 가능한 공간에서 스마트폰, 태블릿 PC와 같은 통신 매체만 가지고 있다면 언제든지 클라우드 서버에 접근할 수 있기 때문이다. 용의자 또는 공범에 의해 디지털 증거가 삭제되는 시점에도 다른 사용자들에 의해 많은 양의 데이터가 저장된다. 따라서 증거가 저장되어 있던 공간이 보존되어 있을 가능성은 희박하다. 위와 같은 이유로 서비스 이용을 제한한다면 이용자의 불편과 서비스 제공자의 이미지에 부정적인 영향을 주며, 금전적 피해까지 발생 될 수 있으므로 연결 케이블 또는 전원을 차단하는 조치는 할 수 없다[9].

3.2.4 대용량

클라우드 서비스 이용자의 디지털 정보는 중앙 집중화된 스토리지 서버에 저장된다. 서비스 제공자는 사용자가 원하는 만큼의 데이터 저장 공간을 제공하고 원활한 서비스를 유지하기 위해 많은 대용량 서버를 운영한다. 따라서 서비스 제공자의 전체 서버를 압수수색할 경우 많은 양의 데이터를 수집하여 저장할 수 있는 공간 확보와 분석에 필요한 시간이 증가하는 문제가 수반된다[10].

3.2.5 접속 권한 획득 실패의 문제

과거에는 서비스 제공자로부터 계정정보를 쉽게 획득할 수 있었지만, 현재는 불가능하다. 이는 2015년 5월 19일에 시행된 개인정보의 기술적·관리적 보호조치 기준 제6조에 따라 정보통신서비스 제공자들이 비밀번호를 복호화할 수 없도록 일방향 암호화되어 저장되기 때문이다. 범죄에 사용된 계정 정보를 획득하는 것이 클라우드 환경에 적합한 디지털 포렌식 모델 제안의 주요 요소가 될 것이다.

3.3 클라우드 환경에 적합한 디지털 포렌식 수사 모델

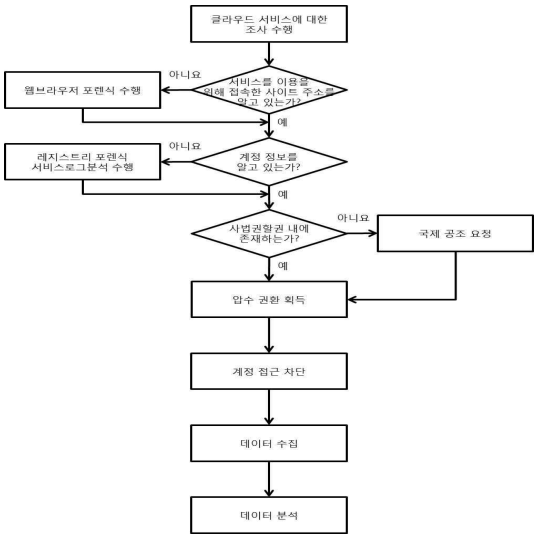
클라우드 환경에서의 기존 디지털 포렌식 수사 절차의 취약점은 데이터의 저장이 개인 단말에서 중앙 집중화된 서버로 이동하면서 발생되었다. 클라우드 서비스 제공자는 많은 이용자의 정보를 저장하기 위해 대용량의 서버들을 운영하며, 그 공간에서 디지털 증거를 찾기 위해 진행되는 압수수색 과정에서 영장주의에 저촉되는 현상이 발생하는 것이다. 또한, 디지털 증거와 관련 없는 다른 사용자의 정보를 분석함으로써 발생되는 과잉압수수색과 개인정보침해 문제, 여러 사람이 동시간대에 접속이 가능한 클라우드 서비스 특성으로 발생되는 문제, 압수 대신에 데이터를 복사할 경우 발생되는 문제들이 있다. 이는 계정 정보를 통해 압수수색을 할 경우 취약점들은 보완이 가능하다. 하지만 클라우드 서비스 제공자로부터 계정 정보 획득은 불가능하다. 새로운 수사 모델은 개인 단말에서 계정정보를 획득할 수 있는 과정을 추가함으로써 앞에서 언급한 문제점들을 해결하였다. 계정을 통한 압수수색 절차는 다음과 같다.

1. 클라우드 서비스에 대한 조사를 수행한다.
2. 클라우드 서비스를 이용하기 위해 접속한 사이트 정보를 알고 있는가?
   2.1 (사이트 정보를 모를 경우) 웹 브라우저 포렌식을 수행한다.
3. 클라우드 계정 정보를 알고 있는가?

3.1 (계정 정보를 모를 경우) 레지스트리 포렌식과 로그 분석을 수행한다.

4. 서비스 제공자가 사법권할권 내에 존재하는가?
   4.1 (사법권할권 내에 존재하지 않을 경우) 국제 공조를 요청한다.
5. 획득한 계정에 대한 압수수색 권한을 획득한다.
6. 계정접근을 차단한다.
7. 해당 계정에 담긴 데이터를 수집한다.
8. 수집된 데이터를 분석한다.

클라우드 시그니처란 해당 시스템이 클라우드 서비스 접속에 사용되었는지 판단할 수 있는 데이터를 의미한다. 이 데이터에는 클라우드 서비스를 이용하기 위해 접속한 사이트 정보와 계정정보가 포함된다. 사이트 정보는 웹브라우저 포렌식으로 획득 가능하며, 계정정보는 레지스트리 포렌식과 로그 분석을 통해서 수집 가능하다[11]. (그림 2)는 클라우드 환경에 적합한 수사 절차를 수사 모델로 표현한 것이다.



(그림 2) 클라우드 환경에 적합한 디지털 포렌식 수사 모델

기존 디지털 포렌식 수사 절차에서 보완된 사항은 다음과 같다. 첫째, 법적으로 일방향 암호화하여 저장되어 있는 계정 정보를 획득할 수 있는 절차를 추가하였다. 클라우드 서비스 이용을 위해 사용된 계정에 대한 압수 권한이 획득된다면 기존 수사 절차의 취약점을 보완할 수 있다. 둘째, 용의자 또는 공범에 의해 디지털 증거를 은닉하거나 삭제·위조·변조하는 것은 쉽게 가능하다. 계정정보를 획득하였다고 하더라도 디지털 증거가 삭제되거나 훼손되었을 우려가 있다. 그래서 계정 접근 차단 절차를 추가하여 용의자 또는 공범에 의한 디지털 증거 인멸에 대한 대책을 보강하였다. 셋째, 공공 클라우드와 사설 클라우드의 수사 절차를 구분하지 않았다. 공공 클라우드는 사용량만큼 요금을 지불한다면 누구든지 이용할 수 있고 사설 클라우드는 기업이나 기관 내에 서비스 환경을 구성하여 직원들만 이용할 수 있게 한 서비스이다[12]. 즉 이용자가 구분될 뿐이지 구축 환경과 원리는 동일하다. 이 두 클라우드 유형에 모두 적용할 수 있는 표준화된 모델을 제시하였다.

<표 3> 기존 수사 모델과 제안된 수사 모델 비교

수사모델 / 취약점	기존 수사 모델 〔그림 2〕	제안된 수사 모델 〔그림 3〕
압수 수색 대상 및 범위	불명확	클라우드 계정
과잉압수수색과 개인정보침해 우려	있다	없다
데이터 복사를 위해 필요한 저장 공간	대용량	저용량
디지털증거 훼손 및 은닉 우려	있다	없다
계정 정보 획득 과정	없다	있다

4. 결 론

최근 보안 안정성과 편리성, 비용 절감 등의 이유로 데이터의 저장 위치가 개인 단말에서 클라우드로

변하고 있으며, 일반 사용자부터 정부 기관, 기업의 이용률도 매년 증가하고 있다. 정보가 중앙 집중화됨에 따라 개인정보 유출, 불법정보 은닉, 보안이 위협되는 사례가 발생되었고, 이전에 비해 피해 규모가 늘어났다. 하지만 기존 디지털 포렌식 수사 절차를 이용하여 클라우드 환경에서 발생하는 사건을 수사하기에는 부족하다. 그래서 클라우드 환경에 적합한 수사모델을 제시하였고 향후 설문조사나 전문가 기법을 활용하여 적합성을 검증하도록 하겠다. 기술이 발전할수록 범죄 수법도 진화된다. 이런 상황에서 제시된 수사모델이 앞으로의 수사 과정에서 도움이 되길 기대해 본다.

참고문헌

[1] 김병일, 서광규, “클라우드 컴퓨팅과 관련된 법적 쟁점에 관한 고찰”, Internet and Information Security, 제3권, 제3호, pp. 49-66, 2012

[2] 한국인터넷진흥원, ‘2015년 인터넷이용실태조사 요약보고서’, 한국인터넷진흥원, 2015

[3] 미래창조과학부 소프트웨어진흥과, ‘공공부분 클라우드 컴퓨팅 도입 수요 조사 결과 공개’ 보도자료, 미래창조과학부, 2017

[4] 이원상, 이성식, 이정환, 탁한용, ‘클라우드 컴퓨팅 환경에서의 사이버범죄와 대응방안 연구‘, 한국형사정책연구원, 2012

[5] 정준현, 이창범, 정관영, 김진환, 고영하, 김현철, ‘클라우드컴퓨팅법 해설서’, 정보통신산업진흥원 ,2015

[6] 고려대학교 디지털포렌식연구센터, ‘디지털 증거 처리 가이드라인’, 고려대학교 디지털포렌식연구센터

[7] 김경도, “압수·수색의 문제점”, 대검찰청, 검찰 통권, 제116호, pp. 276-306, 2005

[8] 조광훈, “디지털 증거의 압수·수색의 문제점과 개선방안”, 서울法學, 제21권, 제3호, pp. 699-738, 2014

[9] 김홍원, “클라우드 스토리지 압수수색 시 문제점과 분석방법에 관한 연구”, 석사학위논문, 서울대학교 융합과학기술대학원, 2015

[10] 박래옥, “클라우드 스토리지의 효율적인 압수·수색을 위한 방안”, 석사학위논문, 서울대학교 융합과학기술대학원, 2016

[11] 이상진, ‘클라우드 환경에 대한 연구’, 국세청, 2016

[12] 정현지, 이상진, “클라우드 컴퓨팅 환경에서의 디지털 포렌식 동향 및 전망”, 情報保護學會誌, 제22권, 제7호, pp. 7-13, 2012.

[저 자 소 개]

이 규 민 (Gymin Lee)

2012년 2월 ~ 현재 호원대학교 사이버수사경찰학부 학생

email : qmlee777@gmail.comr

이 영 숙 (Youngsook Lee)

2009년 ~ 현재 호원대학교 사이버수사보안학부 부교수
2008년 8월 성균관대학교 컴퓨터공학과 공학박사
2005년 2월 성균관대학교 정보보호학과 공학석사
1987년 2월 성균관대학교 정보공학과 공학사

email : ysooklee@howon.ac.kr