클라우드 포렌식을 위한 신뢰성이 보장된 데이터 로깅 구조 연구

박준학, 박준영, 허의남
경희대학교 컴퓨터공학과
{pincomomo, parkhans, johnhuh}@khu.ac.kr

A Study on Trusted Data Logging Structure for Cloud Forensics

Jun Hak Park, Jun Young Park, Eui-Nam Huh
Department of Computer Science and Enginerring, Kyung Hee Univ.

요 약

점차 늘어나는 클라우드 서비스 이용률과 더불어 보안 위협 또한 증가하고 공격 방법 또한 다양해지고 있다. 하지만 클라우드 환경에서 보안사고가 발생했을 시 대응을 위한 조치나 정책은 여전히 미흡한 실정이다. 보안사고 대응을 위한 디지털 포렌식에 대한 연구를 통해 많은 해결 방법이 제시되고 있으나 클라우드 환경에서는 가상화 기술이 적용되어 있어 기존의 방법으로 증거의 수집 및 보관에 대한 무결성 증명이 까다롭다. 본 논문에서는 클라우드 서비스 이용자가 제공자로부터 서비스를 제공받는 클라우드 환경에서 보안사고 사후 대응을 위한 신뢰성 있는 데이터 수집 구조를 제안한다.

1. 서론

클라우드 컴퓨팅은 물리적인 자원을 가상화 기술을 통하여 인터넷이 가능한 환경에서 이용자들에게 IT 자원들을 서비스로 제공하는 기술이다. 클라우드 컴퓨팅은 일상생활에서 많은 사람들이 이용하고 있는 중요기술로 자리매김 했다. 또한 늘어나는 클라우드 사용자 수와 더불어 보안에 대한 관심 또한 높아지고 있다. 클라우드를 위한 많은 보안 솔루션들이 연구가 되고 있지만, 보안사고 사후 조치는 가상화 환경이라는 특징 때문에 기존 디지털 포렌식의 방법을 그대로 적용하기에 어려움이 있다[1]. 또한 클라우드 환경을 서비스 모델별로 분류해 보았을 때 Software-as-a-Service(SaaS)와 Paltform-as-a-Service (PaaS) 환경에서는 일부 시스템 계층에 대한 접근이 불가능하고 해당 계층에 대한 접근 권한은 Cloud Service Provider(CSP)에 있기 때문에 접근이 안 되는 계층에서 발생하는 보안사고 발생 시 필요한 로그 데이터는 CSP와의 사전협의 등의 방법을 통해 제공받을 필요가 있다[2]. 본 논문에서는 클라우드 환경에서 보안사고 발생 시 포렌식 절차를 원활히 수행하기 위해 필요한 데이터 및 로그를 저장하는 구조를 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 클라우드 포렌식과 클라우드 환경에서 포렌식 적용을 위한 관련 데이터의 신뢰성 있는 수집 방법을 연구한 기존 연구를 살펴본다. 3장에서는 관련 연구에서 언급한 내용을 참고하여 Cloud Service Customer(CSC) 와 CSP로 구성된 클라우드 환경에서 신뢰성 있는 데이터 로깅 구조의 위치와 역할에 대해 제안한다. 마지막으로 4장에서는 연구 내용을 최종적으로 정리하고 향후 연구 방향을 제시한다.

2. 관련 연구

1) 클라우드 포렌식

클라우드 포렌식은 클라우드 환경에서 발생한 보안 사고의 사후 대응을 위한 증거 수집부터 법정에서 증거로서의 효력을 발휘하게 하는 통합적인 절차를 뜻한다. 이 과정은 National Institute of Standards and Technology(NIST) 문서[1]에 따르면 디지털 포렌식의 절차는 자료의 수집, 관련 데이터의 분류, 분석 및 조사, 최종적으로 보고하는 4단계의 절차로 구성되어 있다. 디지털 포렌식의 절차를 클라우드 환경에 적용하고자 할 때의 문제점은 클라우드 환경이 CSP로부터 원하는 서비스 혹은 자원을 제공받아 사용하는 아웃소싱 리소스라는 것과 가상화 기술이 적용된 환경이라는 특징 때문에 자료 수집이 어렵다는 것이다. 따라서 해당 환경의 특성을 충분히 고려한 자료의 신뢰성 있는 식별 및 수집 방법이 필요하다.

2) 클라우드 포렌식을 위한 로그 데이터 수집 서비스[3]

클라우드 환경은 CSC가 수집 가능한 로그의 종류가 서비스 환경 및 유형에 따라 다를 뿐만 아니라 수집 및 엑세스 권한이 CSP에 의존적인 특징이 존재한다. Zawoad[3] 는 이와 같은 문제점을 해결하고자 포렌식 조사를 위한 보안 관련 로그를 신뢰성이 보장된 방법으로 수집하는 서비스 모델을 제안하였다. 또한 클라우드 포렌식을 위한 로그 스키마의 구조를 정의하고, 로그 데이터를 주기적으로 수집하고 암호화 하여 일(day) 단위로 압축하여 신뢰성을 보장하는 Proof of Past Log(PPL)의 개념을 제안하였다. 제안하는 서비스는 클라우드 환경에서 포렌식을 위해 수집해야 하는 데이터의 종류 중 VM들 간의 네트워크 패킷 로그만을 대상으로 진행하였다는 한계점이 존재한다.

3. 신뢰성이 보장된 클라우드 포렌식 서비스 구조

앞서 서론에서 언급하였듯이 클라우드 환경에서는 이용하고 있는 서비스의 종류 또는 역할에 따라 접근 및 제어 가능한 범위가 다르기 때문에 Infrastructure-as-a-Service(IaaS) 와 같이 모든 시스템 계층에 접근 및 제어 권한이 CSC에게 있는 경우 외에는 보안사고 발생 시 증거 자료 수집을 위해서 사전에 CSP와의 협의를 통해 제어 및 접근이 불가능한 시스템 계층에서 발생하는 로그 데이터를 수집하는 서비스를 받을 수 있어야 한다. 예를 들어 SaaS 환경에서는 CSC가 주로 웹을 통해 서비스를 이용하기 때문에 어플리케이션 계층 아래에서 발생하는 로그 데이터들은 접근권한이 CSP에게 존재한다. 이때 CSP가 의도적으로 해당 자료를 은폐하거나 기록하지 않을 경우 CSC는 수사에 필요한 데이터를 구할 수 없게 된다. 따라서 서비스 사용 전 CSC와 CSP간 Service Level Agreement(SLA)를 통해 사고발생 시 증거 자료로 사용될 수 있는 로그데이터의 종류와 수집 및 저장 방법을 명시하여야 한다.

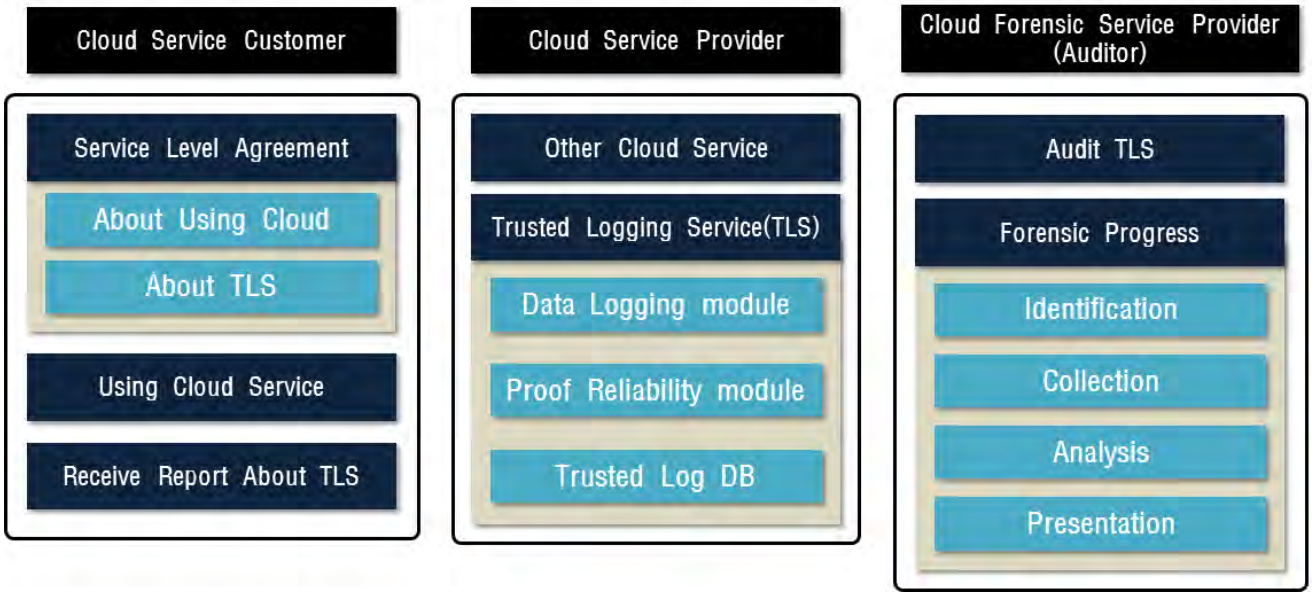
클라우드 환경에서 신뢰성 있는 로그 데이터 수집 및 제공 서비스를 제공하는 시스템의 구조도는 (그림 1)과 같다. (그림 1)의 시스템 구조는 클라우드 서비스를 이용하는 CSC, 클라우드 서비스를 제공하는 CSP, 클라우드 환경에서 수집된 증거 자료로 포렌식 절차를 수행하는 Cloud Forensic Service Provider(CFSP)의 총 세 가지로 분류된다. 각 시스템을 구성하는 역할에 따른 설명은 다음과 같다.

1) Cloud Service Customer(CSC)

CSC는 CSP에게 SLA를 통해 이용하고자 하는 서비스에 관한 서비스 품질관련 보상에 대한 규정 외에도 보안사고 발생 시 포렌식 수사 진행을 할 수 있도록 수집해야 하는 로그 데이터의 종류와 방법을 사전에 협의하여야 한다. 또한 CSC는 해당 데이터가 올바르게 기록되고 있는지 CSP로부터 저장되고 있는 데이터의 정보를 CFSP에게 주기적으로 리포트 형식으로 보고를 받아 확인할 수 있다.

2) Cloud Service Provider(CSP)

CSP가 자체적으로 CSC가 요청한 로그 데이터를 수집하여 보관하는 절차를 진행하게 될 경우 의도적 또는 부주의로 인해 의해 특정 데이터를 기록하지 않거나, 삭제해 버리는 경우가 발생할 수 있다. 이 문제를 해결하기 위해 해당 환경에서 발생하는 데이터의 수집 및 저장 행위를 서드파티 CSP 환경에서 수행하게 된다면 신뢰성은 보장받을 수 있으나 본 논문에서 제안하는 구조는 해당 서비스 환경에서 발생하는 로그 데이터의 저장을 서비스를 제공하는 CSP가 수행하고 이에 따른



(그림 1) 제안하는 클라우드 포렌식을 위한 데이터 로깅 서비스 구조도

무결성의 검증은 CFSP에서 이루어지는 구조임을 전제로 한다.

신뢰성 있는 로그 저장 서비스(TLS)의 경우 로그 데이터를 저장하는 모듈과 저장 및 보관 시 해당 데이터의 신뢰도를 검증하는 모듈, 그리고 신뢰성 검증을 마친 데이터들을 보관하는 DB로 구성되어 있다. 신뢰성 검증을 마친 DB는 보안사고 발생 시 CFSP에서 포렌식 절차를 진행할 때 API등의 방법을 통해 제공하여 증거자료로서 사용하게 된다.

3) Cloud Forensic Service Provider(CFSP)

CFSP는 CSP가 제공하는 클라우드 환경 내에서 CSC가 기록을 요청한 로그 데이터들이 올바르게 기록되고 있는지를 DB에 저장하는 과정 전에 검사하여 저장 여부를 결정한다. 앞서 언급한 바와 같이 CSP내에서 발생하는 로그 데이터에 대한 신뢰성 검증을 CSP내에서 진행하는 것은 자체적으로 특정 데이터를 은닉 및 제거할 수 있는 가능성이 존재한다. 따라서 CSP가 로그 데이터 저장 시 CSP내 TLS의 신뢰성 검증 절차뿐만 아니라 CFSP의 감사(Audit TLS) 기능을 통해 해당 절차를 추가적으로 검증한다. 검증 절차를 마친 로그 데이터는 최종적으로 CSP 내의 DB에 저장되어 보안사고 발생 시 포렌식 절차 중 식별 및 수집 단계에서 사용된다. 또한 주기적으로 CSC에게 본 서비스에 대한 리포트를 제공한다.

클라우드 포렌식 서비스 과정에서 CSC는 보안사고가 발생하였을 시 사후 대응을 위해 클라우드 포렌식 서비스를 CSP에게 요청한다. 이후 CSP는 CFSP에게 서비스를 요청하고 CSC와 CFSP의 협의를 통해 결정된 수집해야 하는 로그 데이터 목록을 받아 TLS를 이용하여 로그를 수집하게 된다. 해당 서비스가 시작이 되고나면 CSC는 클라우드 포렌식을 위한 별다른 추가 절차 없이 CSP로부터 제공받는 서비스를 이용하며, 보안사고 사후 대응을 위한 로그 데이터가 올바르게 수집되고 있는지 주기적으로 리포트를 받게 된다. CSP는 CSC가 요청한 서비스를 제공함과 동시에 해당 환경에서 발생하는 로그 데이터 중 클라우드 포렌식에 필요한 데이터를 저장한다. CFSP는 보안사고 발생 시 CSP로부터 제공받은 데이터를 이용하여 포렌식 절차를 진행하며, 사고발생 전에도 주기적으로 CSP에서 데이터를 올바르게 저장하고 있는지 검증하는 역할을 수행한다.

데이터를 제공받아 포렌식 절차를 수행할 때 클라우드 환경의 특징 때문에 기존 디지털 포렌식의 방법을 적용할 수 없는 절차는 식별(Identification)과 수집(Collection) 부분이며, 이후 분석(Analysis)과 발표(Presentation) 과정은 디지털 포렌식과 일치한다[1]. 따라서 CSC가 클라우드 포렌식을 위한 신뢰성이 보장된 로그 데이터 기록 서비스를 CSP에게 요청할 경우 사용하고 있는 서비스의 종류에 따라 CSP 뿐만 아니라 클라우드 포렌식 서비스 제공자와의 충분한 협의를 통해 SLA 항목을 선정해야 한다. CFSP는 클라우드 포렌식 절차를 수행함과 동시에 CSP에서 로그 데이터가 위변조 및 손실 없이 저장되고 있는지 감시하는 역할을 겸하고 있기 때문에 국제표준 ISO/IEC 17789[4]에서 정의된 역할 중 Cloud Service Partner(CSN) 의 세부역할인 Auditor가 수행할 수 있다.

4. 결론

본 논문에서는 CSC가 CSP의 서비스를 이용하는 단일 클라우드 환경에서 보안사고 발생 시 포렌식을 수행하기 위해 필요한 역할인 CFSP의 개념과 서비스 절차 및 역할 간 고려사항에 대해 연구하였다. 본 연구를 통해 클라우드 환경에서 포렌식을 서비스 형식으로 제공하는 구조에 대한 참조 모델로써 사용될 수 있는 효과를 기대해 볼 수 있다. 향후 연구로는 무결성을 보다 효율적으로 검증할 수 있는 절차와 로그 데이터의 종류에 따른 수집 방법 및 저장 스키마를 연구할 것이다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2017-2013-0-00717)

참고문헌

[1] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,” NIST Special Publication, pp. 800 - 86, 2006.

[2] Josiah Dykstra, Alan T. Sherman, “Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques“, Digital Investigation 9, 2012

[3] Zawoad et al., “SecLaaS: Secure Logging-as-a-Service for Cloud Forensics”, Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, pp. 219-12, 2013

[4] ISO/IEC, “Final Revised Text of ISO/IEC 17789 - Information Technology - Cloud Computing - Reference Architecture for ITU_T SG3 Review”, 2014.5