http://dx.doi.org/10.14400/JDC.2014.12.12.303

신뢰되는 DRM 클라우드 서비스를 위한 책임 추적성 분석 및 모니터링 툴 설계

이혜주*, 서창호**, 신상욱***
숭실대학교 컴퓨터학부*, 공주대학교 응용수학과**, 부경대학교 IT융합응용공학과***

Analysis of Accountability for Trust DRM Cloud Service and Design of Monitoring Tool

Hyejoo Lee*, Changho Seo, Sang Uk Shin*****
School of Computing, Soongsil University*
Dept. of Applied Mathematics, Kongju National University**
Dept. of IT Convergence and Application Engineering, Pukyong National University***

요 약 클라우드 사용자들에게 책임 있는 서비스를 제공하는 클라우드 서비스의 책임 추적성(accountability)은 서비스 정책 준수, 모니터링 및 감사(auditing), 로그 정보 기록(logging) 등과 같은 여러 가지 기술을 적용한다. 궁극적으로 데이터 처리, 서비스 제공 과정에서 발생되는 여러 가지 문제들에 대해 누가 책임이 있는지를 판단함으로써 신뢰되는 클라우드 서비스를 제공하는 것을 목적으로 한다. 먼저, 부가가치가 높은 콘텐츠 서비스 제공 시에 안전하고 신뢰되는 DRM 클라우드 서비스를 제공하기 위해 본 논문에서는 콘텐츠 및 DRM 클라우드 서비스 체인을 이루는 클라우드 에코 시스템을 제시한다. 또한 콘텐츠 소유자와 콘텐츠 사용자의 DRM 클라우드 서비스에 대한 요구사항을 분석하고, 책임 추적을 위해 기록해야 할 로그 정보 및 모니터링 툴 구조를 제안한다.

주제어 : 클라우드 컴퓨팅, 책임 추적성, 디지털 저작권 관리 기술, 콘텐츠 서비스, 모니터링

Abstract The accountability of cloud service which provides the cloud users with accountable services applies various technologies such as the compliance of service policy, monitoring and auditing, logging, and others. It ultimately intends to provide trustworthy cloud service by determining who is accountable for various problems happened during data processing and service offering. In this paper, we propose a cloud ecosystem formed from the chain of content and DRM Cloud service in order to offer secure and trust DRM cloud service when providing high value-added content service. Besides this, we analyse the requirements of cloud services for content owners and users and then propose some logging information to be recorded for trace of accountability and a structure of tool for monitoring.

Key Words : Cloud computing, Accountability, Digital rights management, Content Service, Monitoring

* 이 논문은 2011년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No. 2011-0029927)
Received 13 October 2014, Revised 17 November 2014
Accepted 20 December 2014
Corresponding Author: Sang Uk Shin
(Pukyong National University)
Email: shinsu@pknu.ac.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

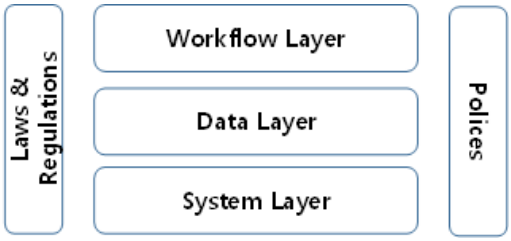
1. 서론

현재 기업과 개인 사용자를 대상으로 클라우드 서비스를 이용한 다양한 서비스 제공이 점차 증가하고 있다. 특히 부가가치가 높은 콘텐츠 서비스 환경은 점점 클라우드 서비스로의 이동이 활발하게 이루어지고 있다[1, 2, 3, 4, 5]. 안전하고 신뢰성 있는 클라우드 콘텐츠 서비스를 제공하기 위해서는 콘텐츠 보호 기술, 콘텐츠 서비스가 어디에서, 어떻게 처리되는지에 대한 서비스 정책의 제공과 준수, 그리고 발생되는 문제에 대한 책임 소재 등에 관한 서비스 신뢰성 등이 주요 요소가 된다. 이를 위하여 콘텐츠 보호 기술은 라이선스 관리, 도메인 관리, 콘텐츠 암호화 등을 포함한 DRM(digital rights management)을 적용하고, 클라우드 서비스에 대한 신뢰성을 위해서는 클라우드 서비스의 책임 추적성(accountability)을 각각 적용할 수 있다. 여기에서 책임 추적성이란 시스템 내의 각 개인을 유일하게 식별하여 정보 보호 규칙을 위반한 개인을 추적하여 그에 대한 책임을 지게 하는 것으로, 콘텐츠 서비스 영역에서의 책임 추적성은 콘텐츠 소유권자의 저작권이 잘 보호되고 있는지, 콘텐츠 사용자의 사용권한이 올바르게 제공되고 있는지에 대한 증거를 제공하고 사용권한이나 저작권 침해가 발생되었을 때 책임 소재를 판단하여 클라우드 사용자의 신뢰를 확보하고자 하는 것을 의미한다. 이를 위해 콘텐츠의 등록에서부터 콘텐츠의 사용에 이르기까지, 즉 클라우드 콘텐츠 서비스 및 DRM 서비스 체인 전반에 걸쳐 책임 추적을 위한 복잡한 처리가 제공되어야 한다.

본 논문에서는 클라우드 사용자와 클라우드 제공자 간의 관계를 기반하여 콘텐츠와 DRM 클라우드 서비스를 제공하는 클라우드 에코 시스템 모델을 정립하고, 클라우드 상에서 신뢰되는 콘텐츠 서비스와 DRM 서비스를 제공하기 위해 서비스 체인 내 참여자들의 책임 추적성을 분석하고자 한다. 특히 콘텐츠 보호를 위한 DRM 서비스에 초점을 두고 안전한 콘텐츠 서비스를 위한 책임 추적성에 논의한다. 논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구로써 클라우드 책임 추적성에 대해 간단하게 소개한다. 그리고 3장에서는 DRM 클라우드 서비스와 콘텐츠 클라우드 서비스로 구성된 클라우드 에코 시스템에 대한 소개와 클라우드 에코 시스템을 구성하는 클라우드 사용자와 제공자 간의 관계를 정립하고, 신뢰되는 클라우드 서비스를 위한 참여자 요구사항을 분석한다. 그리고 4장에서는 이러한 책임 추적성을 지원하기 위한 모니터링 툴 설계에 대해 논의한다. 마지막으로 결론으로써 5장에서는 향후 연구 내용에 대해 논의한다.

2. 관련기술

최근의 DRM 기술은 모바일, PC, TV 등 다양한 스마트 단말을 대상으로 콘텐츠를 서비스하는 환경을 고려하여 개발되고 있다. 예를 들어 홈 내 가족 구성원들 간의 콘텐츠 공유를 지원하는 UltraViolet 에코 시스템[6], 마이크로소프트의 PlayReady 에코시스템[7], 개방형 DRM 기술을 지향하는 Marlin DRM 시스템[8], 그리고 모바일 환경을 고려한 OMA DRM[9] 등 복수의 플랫폼을 고려하여 상호운용 가능하도록 기술이 개발되어지고 있다. 우리는 이와 같은 DRM 주요 기능인 라이선스 관리, 콘텐츠 패키징, 도메인 관리 등을 클라우드 환경에서 서비스로 제공하는 DRM 클라우드 서비스를 제안하였다[10, 11]. 컴퓨팅 리소스를 임대하여 이용하는 클라우드 서비스의 특성 상 사용자들은 자신의 데이터가 안전하게 저장, 전송 및 처리되는가에 대해 신뢰되는 클라우드 서비스를 요구하게 된다. 최근 신뢰되는 클라우드 서비스를 제공하기 위한 책임 추적성(accountability)에 관해 많은 연구가 활발하게 이루어지고 있다. 책임 추적성은 클라우드 상의 중요한 사용자 데이터의 사용을 통제하고 관리하고, 그에 대한 책임을 지도록 함으로써 신뢰되는 클라우드 서비스를 제공하는 것으로, 클라우드 서비스 환경에서 서비스 정책 준수(compliance)[12], 안전한 로그 정보 기록(logging)[13], 모니터링 및 감사(auditing) 등에 관하여 연구되고 있다[14, 15]. 실제 책임 추적성은 클라우드 서비스 상에 이루어지는 행위와 주체를 증거로써 기록함으로써 이루어진다. 따라서, 증거로써 제공하기 위한 데이터의 추적 방식과 기록에 대한 여러 가지 연구가 이루어지고 있다[12, 16, 17, 18, 19]. 이 중에서, Ko 들은 보다 체계적인 분석을 위해 책임 추적성을 [Fig. 1]과 같은 추상화된 계층으로 분류하여 제안하였다[16].



[Fig. 1] Abstraction layer of accountability

[Fig. 1]에 나타난 바와 같이 시스템 계층에서는 운영체제, 파일 시스템, 그리고 클라우드 내 네트워크 사용에 대한 로그 정보를 기록함으로써 클라우드 내의 가상 및 물리적 서버에 대한 상태들을 추적할 수 있게 된다. 데이터 계층에서는 데이터의 출처, 수집, 생성, 사용 등 데이터의 히스토리를 추적하여 데이터의 생성과 획득, 포함된 프로세스들의 유효성, 비정상적 행위 검출 등을 수행할 수 있게 한다. 워크플로우 계층은 클라우드 내의 소프트웨어 서비스의 감사 추적과 관련 데이터에 주목한다. 즉 클라우드 어플리케이션의 적절한 통제를 보증하고 지속적인 감사와 비즈니스 프로세스를 구성한 서비스들의 책임 추적성을 관리한다.

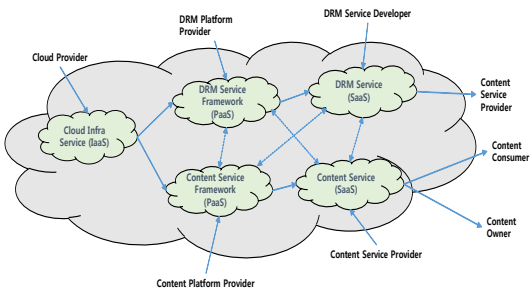
제공되는 클라우드 서비스는 가상 머신에서 수행되고 처리되기 때문에 책임 추적성 기능은 가상 머신(virtual machine, VM)과 가상 머신이 동작되는 물리적 머신(physical machine, PM) 상에 가상 머신에 대한 모니터링, 로그 정보의 기록, 물리적 머신(physical machine)과의 연계를 고려한 기술이 적용된다[20, 21]. 이러한 가상 머신을 고려한 모니터링 기술은 중요성에도 불구하고 많은 연구가 이루어지고 있지 않다. 그 중에서 Ko의 Flogger 방식[20]은 데이터 계층에서의 책임 추적성 기능을 위한 모니터링 방법을 제안하는 것으로 VM 내 파일 관련 처리를 인터셉트하여 다음과 같은 로그 정보를 기록하게 된다.

- VM 내 접근한 파일 이름 및 경로
- VM 내 파일 접근 날짜 및 시간
- VM IP 어드레스
- VM MAC 어드레스
- 머신 유형(VM 또는 PM)
- 접근 파일의 파일 소유권자의 UID, GID
- 파일에 접근한 프로세서 소유자의 UID, GID
- 접근한 파일에 취해진 동작, 즉 파일 생성, 읽기, 쓰기, 네트워크 전송, 삭제
- 목적 머신의 ID 어드레스
- 목적 머신에 보내는 패킷 내용

또한 Yao들은 SOA(service oriented architecture) 기술을 기반으로 하나 이상의 비즈니스 서비스 도메인 내에서 책임 추적성을 제공하는 방법을 제안하였다[15]. 즉, SLA(service level agreement)를 준수하도록 BPEL(business process execution language)를 이용하여 비즈니스 프로세스 간 정확한 상호 동작을 정의하고 이러한 동작에 대한 정보들을 기록하고, 모니터링 및 감사 처리를 수행함으로써 책임 있는 서비스를 제공하는 것을 목적으로 하였다. 현재 EU프로젝트인 A4Project는 책임 추적성 프레임워크와 툴을 개발하여 데이터 사용에 대한 제어 및 투명성, 준수와 감시, 그리고 윤리적 책임성을 제공하는 것을 목적으로 활발하게 활동 중이다[22, 23].

3. 콘텐츠 및 DRM 클라우드 서비스의 책임 추적성 분석

DRM 클라우드 서비스의 책임 추적성을 제공하기 위해서 콘텐츠 서비스를 위한 콘텐츠 등록에서 콘텐츠의 사용에 이르기까지 서비스 과정 전반에 걸쳐 각 클라우드 서비스가 어떻게 관련되어 있는지를 분석하기 위해 [Fig 2]와 같이 콘텐츠 및 DRM 클라우드 서비스 체인으로 구성된 클라우드 에코 시스템(이하 클라우드 에코 시스템)을 제시한다.



[Fig. 2] Cloud Ecosystem with Content and DRM Cloud Service Chain

[Fig. 2]에 표시된 바와 같이 이 클라우드 에코 시스템은 클라우드 서비스 모델 개념인 IaaS, PaaS, SaaS까지 구성된 서비스 체인을 가지고 있다. 즉 IaaS를 제공하는 클라우드 인프라 서비스, PaaS를 제공하는 DRM 서비스 프레임워크와 콘텐츠 서비스 프레임워크, 그리고 SaaS를 제공하는 DRM 서비스와 콘텐츠 서비스로 각각 구성된다. 각 서비스의 제공자 및 사용자 역할을 수행하는 클라우드 에코 시스템의 참여자에 대한 자세한 설명을 <Table 1>에 기술한다.

〈Table 1〉 Entities of Cloud Ecosystem

Entity	Definition	Role	Service
Cloud Provider	Service provider, who provides cloud infrastructure for environment of cloud computing such as storage, network and so on.	Provider	Cloud infra-service
Content Platform Provider	Service provider, who provides development environment for various content processing such as some libraries of content coding, compression, etc.	Provider	Content service platform
DRM Platform Provider	Service provider, who provides development environment such as DRM-related libraries for license management, content packaging, etc.	Provider	DRM service platform
Content Service Provider	Content service provider, who plans various content service scenarios and distributes the contents as well as consumer who uses DRM service for content protection	Provider/ User	Content Service
DRM Service Provider	Service provider, who develops and provides DRM-related services such as license management, key management, etc.	Provider	DRM service
Content Consumer	End-user, who purchases and consumes the content using content service.	End-user	
Content Owner	End-user in side of content service business, who uses the content service to distribute the content.	End-user	

여기서 콘텐츠 서비스 제공자나 DRM 서비스 제공자는 자신이 IaaS 또는 PaaS 제공자가 될 수 있다. 이러한 서비스로 구성된 클라우드 에코 시스템에서, 콘텐츠 플랫폼 제공자 및 DRM 플랫폼 제공자는 클라우드 인프라 서비스를 기반하여 콘텐츠 서비스를 위한 다양한 API, 컴포넌트, 개발 통합 환경 등 PaaS 서비스를 구축한다. 예를 들어 OMA DRM의 기능을 위한 각종 라이브러리, 개발 툴 등을 DRM 서비스 플랫폼에 구축하여 OMA DRM 기능을 탑재할 단말의 제조사에게 OMA DRM 플랫폼을 클라우드 서비스를 이용하여 DRM 모듈을 구현할 수 있게 한다.

클라우드 에코 시스템을 이용하는 서비스의 최종 사용자는 콘텐츠 서비스를 위한 비즈니스 측면과 콘텐츠 서비스를 사용하는 사용자 측면으로 분류할 수 있다. 비즈니스 측면에서의 최종 사용자는 콘텐츠 소유자이고, 사용자 측면에서의 최종 사용자는 콘텐츠 사용자이다. 따라서 최종 사용자인 콘텐츠 소유자와 콘텐츠 사용자는 신뢰하는 클라우드 서비스를 받기 위해 여러 가지 사항을 클라우드 서비스에게 요구하게 된다. 또한 DRM 서비스의 책임 추적성에 대한 사용자 요구사항을 DRM 서비스에 적용하기 위해 서비스에 대한 사용자의 요청 및 처리 이벤트를 실시간 모니터링하고 이에 해당하는 로그 정보를 기록해야 한다. 이때 사용자의 요구사항을 Ko의 추상화 계층에 맵핑하여 사용자 요구사항에 따른 책임 추적 내용을 계층별로 분석한다.

먼저, 콘텐츠 소유자의 경우에 자신의 콘텐츠를 배포하여 금전적인 이득을 얻는 것을 목적으로 한다. 이를 위하여 콘텐츠 서비스 제공자에게 다음과 같은 사항을 요구한다.

- 요구사항 1: 콘텐츠 배포를 위해 자신과 계약한 콘텐츠 서비스 제공자가 콘텐츠를 계약대로 배포하기를 원한다. 예를 들어 콘텐츠 소유자가 콘텐츠 사용 기간과 횟수를 제한하여 콘텐츠 사용자들이 자신의 콘텐츠를 사용하게 하는 서비스를 제공하도록 콘텐츠 서비스 제공자와 계약했다면, 콘텐츠 서비스 제공자가 이를 위반하지 않고 정확하게 배포되기를 원하게 된다.
- 요구사항 2: 콘텐츠 소유자는 자신의 콘텐츠를 배포하여 콘텐츠 소유권에 대한 금전적인 이익을 얻고자 한다. 따라서 콘텐츠 소유자는 콘텐츠 판매에 따른 이득이 적절하게 자신에게 분배되기를 원한다.
- 요구사항 3: 현재 콘텐츠 서비스가 가능한 최신 보

안 기술들을 이용하여 자신의 콘텐츠를 적절하게 보호하기를 원한다. 이에 DRM 서비스가 요청될 때마다 적용되는 DRM 서비스에 대한 내역을 요구함으로써 적절한 DRM 기술 적용에 대해 신뢰할 수 있다.

이러한 요구사항에 대한 책임 추적성을 제공하기 위해 Ko의 계층으로 분류하여 수행하여야 할 항목을 <Table 2>에 나타내었다.

〈Table 2〉 Accountability for the content owner

Layer / Req.	Workflow	Data	System
Req. 1	- Request of the content purchase - Request of license acquisition	- Usage rights of the content - Information about content consumer and device - Date and time - Information about license service - Network information	- File creation (license) - File creation (content) - Network access
Req. 2	- Request of the content purchase - Request of the payment	- Content consumer's information - Purchase information - Payment information (Credit card, transfer, etc.) - Date and time - Network information	- Network access
Req. 3	- Request of the DRM service	- DRM service history(DRM service type, DRM technology information, DRM service provider's information, etc.)	

<Table 2>의 요구사항 1에 대해 콘텐츠 구매 및 라이선스 발급 서비스 프로세스의 상태에 대해 지속적인 모니터링을 수행하고, 요청한 콘텐츠 사용권한을 비롯한 여러 가지 주요 데이터를 기록한다. 또한 시스템 계층에서는 서비스 결과로 생성된 콘텐츠 및 라이선스 파일의 생성에 대한 정보, 네트워크 처리에 관한 로그 정보를 기록한다.

두 번째로, 콘텐츠 사용자의 경우에 정당하게 구매한 콘텐츠의 사용권한이 정확하게 시행되어 자신의 사용권한이 보호받기를 원한다. 이를 위하여 콘텐츠 서비스 제공자에게 다음 사항을 요구한다.

- 요구사항 1: 콘텐츠 사용자는 자신이 구매한 콘텐츠의 사용 권한이 제공되는 콘텐츠 서비스에 부합하여 올바르게 제공되기를 원한다. 예를 들어 콘텐츠 사용자가 콘텐츠 재생 횟수 제한이 있는 고화질 스트리밍 서비스를 구매하였다면, 콘텐츠 재생 횟수가 정확하게 카운트되기를 원한다.
- 요구사항 2: 콘텐츠 사용자는 자신이 구매한 콘텐츠에 대한 불법 배포의 근원으로 콘텐츠 서비스 제공자로부터 부당하게 지목 당하지 않기를 원한다. 가령 악의를 가진 다른 사용자가 부당한 방법으로 자신에 대한 정보(ID)를 획득한 후 이를 이용하여 콘텐츠를 불법적으로 배포하였을 경우 자신의 무죄를 주장할 수 있기를 원한다.

이러한 요구 사항에 대해 <Table 3>과 같은 책임 추적성 항목을 정의할 수 있다.

〈Table 3〉 Accountability for the content consumer

Layer / Req.	Workflow	Data	System
Req. 1	- Request of content use (Playback, move, share, etc)	- Usage rights of the content - Date and time - Device information	-File modification (License) -File Rad/Copy/ Delete(Content) -Network access
Req. 2		- log-in information - Network information	-Network access

<Table 3>의 요구사항1에 대해, 워크플로우 계층의 콘텐츠 사용(재생, 이동, 공유 등)과 같은 서비스 프로세스를 지속적으로 모니터링하고, 이러한 프로세스가 실행되면 요청한 콘텐츠 사용권한에 대한 정보, 날짜 시간, 그리고 해당 서비스가 요청된 단말의 정보들을 로그 기록한다. 또한 시스템 계층에서는 사용권한의 변경 상태, 또는 복사 및 이동에 대한 정보, 네트워크 접근에 대한 정보도 기록한다.

콘텐츠 서비스 제공자는 최종 사용자는 아니지만, 콘텐츠 서비스를 제공하는 제공자이면서 동시에 DRM 서비스를 사용하는 사용자 역할을 수행한다. 즉 콘텐츠를 안전하게 배포하고 보호하기 위해 DRM 서비스 제공자들이 서비스하는 DRM 서비스를 선택, 이용하게 된다.

이에 콘텐츠 서비스 제공자는 DRM 서비스를 사용하는 사용자로써 다음과 같은 사항을 DRM 서비스 개발자에게 요구한다.

- 요구사항 1: 제공되는 DRM 기능이 DRM 관련한 위협들에 적절하게 대응되어 업데이트되기를 요구한다.
- 요구사항 2: 콘텐츠가 불법 배포가 되었을 때 콘텐츠 서비스 상의 문제인지 또는 서비스되는 DRM 서비스 상의 문제로 발생되었는지에 대해 알기를 원한다.

이와 같은 요구사항을 만족하기 위해 콘텐츠 서비스 제공자에 대한 책임 추적성 항목은 <Table 4>와 같이 정의할 수 있다.

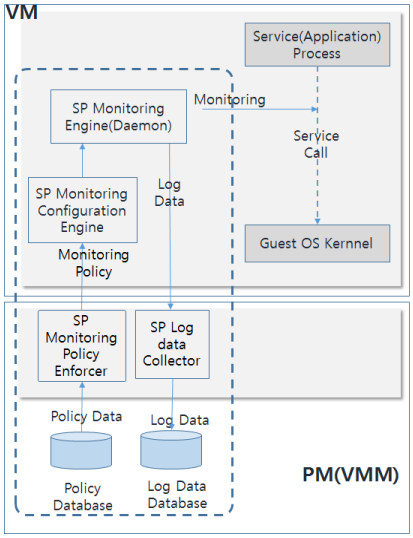
〈Table 4〉 Accountability for the content service provider

Layer / Req.	Workflow	Data	System
Req. 1	- DRM Service update	- DRM service update history - Date and time	- Network access
Req. 2	- Request of the content service - Request of the DRM service	- Content service history - DRM service history	- Network access

<Table 4>의 요구사항1에 대해 DRM 서비스 제공자는 서비스되는 DRM 기술을 업데이트하는 경우 상세한 내역을 기록하여 발생되거나 발생 가능한 위협에 대해 적절하게 대응하고 있음을 콘텐츠 서비스 제공자에게 통지하게 된다. 또한 요구사항 2의 경우, 콘텐츠 서비스 내역과 DRM 서비스 내역에 대한 정보들을 기록함으로써 두 정보를 각각 비교, 분석하여 불법 배포된 해당 콘텐츠에 대한 책임을 지우게 된다.

4. DRM 클라우드 서비스 모니터링 툴 구조 설계

Ko 방식은 시스템 계층에서 파일기반 모니터링을 수행하여 로그 정보를 기록하는데 본 장에서는 이러한 데이터 책임 추적성을 기반으로 DRM 클라우드 서비스에 대한 신뢰성을 제공하기 위해 서비스 중심의 책임 추적성을 제공하기 위한 모니터링 툴 설계를 목적으로 한다. DRM 클라우드 서비스 모니터링 툴은 [Fig. 3]에 표시된 바와 같이, 모니터링 정책 설정 및 시행, 그리고 모니터링과 로그 데이터의 수집 등의 기능을 수행하는 4개의 주요 모듈로 구성된다. 각 모듈에 대한 상세 기능을 기술하면 다음과 같다.



[Fig. 3] Structure of Monitoring Tool for DRM Cloud

- SP 모니터링 정책 시행기(SP-MPE, service process-monitoring policy enforcer): DRM 클라우드 서비스의 PM 내에 배치 가능한 전체 DRM 서비스 프로세스에 대한 모니터링 정책을 정의하고 아래에 기술한 SP 모니터링 정책 설정 엔진에 의해 이해되고 처리 가능한 언어로 기술된 정책 설정(policy configuration) 파일을 생성한다.
- SP 로그 데이터 수집기(SP-LDC, service process-log data collector) : DRM 클라우드 서비스의 PM 내에서 실행되는 다수의 VM에서 동작되는 서비스 프로세스의 모니터링에 의한 결과인 로그 데이터를 수집하고 관리하는 기능을 제공한다. 이러한 로그 데이터는 향후에 감사(auditing)에 의해 책임 추적성을 분석하기 위한 증거를 수집하기 위한 데이터 기초가 된다.

- SP 모니터링 설정 엔진(SP-MCE, service process-monitoring configuration engine): DRM 클라우드 서비스의 PM 내 SP-MPE로부터 설정된 정책 설정 파일을 입력받아 이를 분석하여 SP-ME가 해당 서비스에 대한 동작을 모니터링을 수행할 수 있도록 관리한다.
- SP 모니터링 엔진(SP-ME, service process-monitoring engine) : DRM 클라우드 서비스가 동작되는 개별 VM 상의 서비스 프로세스를 모니터링하는 데몬(daemon) 프로세스이다.

이러한 구조를 가진 모니터링 툴의 동작 단계는 다음과 같이 이루어진다.

- 단계 1: 클라우드 서비스 제공자 및 사용자는 서비스에 대한 계약을 통해 모니터링 정책을 설정한다.
- 단계 2: 클라우드 서비스 제공자는 계약에 의해 설정된 모니티링 정책을 SP-MPE에 사용자 인터페이스를 통하여 입력한다. 입력된 모니터링 정책은 정책 기술 파일로 기술된다.
- 단계 3: 동작되는 PM에 해당 서비스가 제공되는 VM이 배치되어 실행되면 데몬 프로세스로써 SP-ME가 실행된다. 이때 SP-ME는 설정된 정책을 획득하기 위해 SP-MCE를 실행시킨다.
- 단계 4: SP-MCE는 통신을 통해서 PM 내 SP-MPE에 VM 내 서비스에 대한 정보를 전달하고 해당 VM에 대한 정책 기술 파일을 전송받아서 이를 분석하여 SP-ME에게 모니터링 할 프로세스에 대한 정보를 전달한다.
- 단계 5: 프로세스에 대한 정보를 전달받은 SP-ME는 해당 프로세스의 실행, 상태 등을 모니터링하면서 SP-LDC에 로그 정보를 전송한다.
- 단계 6: PM 내 SP-LDC는 SP-ME로부터 로그 데이터를 입력받아 로그 데이터 저장소에 저장한다.

제한한 모니터링 툴은 이 외에도 다음과 같은 사항이 고려되어야 한다.

- [Fig. 3]에 나타난 바와 같이 하나의 PM 내에는 다수의 VM이 실행되기 때문에 SP-MPE 및 SP-LDC는 PM내 가상 머신 관리자(VMM, virtual machine management) 내에 포함되어 PM 내의 전체 VM을 관리해야 한다.
- 본 모니터링 툴 구조에서는 포함되지 않았지만, 추가로 클라우드 서비스를 구성하는 다수의 물리적 서버 전체에 대해 모니터링을 제어하고 관리할 수 있는 통합 모니터링 관리 기능이 포함되어야 한다.
- DRM 클라우드 서비스는 다수의 서비스들이 비즈니스 체인을 이루며 제공되기 때문에 이러한 비즈니스 프로세스에 대한 고려도 이루어져야 한다. 가령, 콘텐츠 등록 시 콘텐츠 패키징 서비스는 단순히 콘텐츠 암호화만 수행되는 것이 아니라 키 관리 서비스도 포함되어야 한다. 따라서, 콘텐츠 패키징 서비스와 키 관리 서비스 간 관련성도 고려해서 책임 추적을 위한 모니터링 정책을 설정하고 이를 모니터링해야 한다.

5. 결론

지금까지 안전한 콘텐츠 서비스를 위한 DRM 클라우드 서비스의 책임 추적성을 제공하기 위해 콘텐츠 및 DRM 클라우드 서비스를 위한 클라우드 에코 시스템과 클라우드 에코 시스템의 사용자인 콘텐츠 소유자, 콘텐츠 사용자, 그리고 콘텐츠 서비스 제공자의 책임 추적을 위한 요구사항을 분석하였다. 분석된 요구사항을 기반으로 책임 있는 서비스를 위해 어떠한 내용을 모니터링하고 로그 정보를 기록해야 하는지를 3개의 계층으로 분류하여 기술하였다. 또한 이러한 내용을 클라우드 에코 시스템에 적용하기 위해 DRM 클라우드 서비스 모니터링 툴에 대한 구조를 설계하고 동작 단계에 대해 기술하였다. 이러한 모니터링 툴을 이용함으로써 클라우드 DRM 서비스에 대한 책임 추적성을 제공하여 콘텐츠 소유자의 소유권과 콘텐츠 사용자의 사용권한을 보호하고 클라우드 서비스에 대한 신뢰성을 확보함으로써 클라우드 서비스 발전에 기여할 수 있을 것이다. 그러나, 이를 위해서 정책 준수를 위한 자동화 방법, 프로세스에 대한 보다 상세한 모니터링 방법, 그리고 책임 추적을 위해 로그 기록 정보를 분석하는 감사(auditing) 방법 등 다양하고 복잡한 기술들이 요구된다. 따라서 향후 연구 과제로써 이러

한 기술들에 대한 연구 및 개발을 수행하고 이를 책임 추적성을 위한 모니터링 툴에 적용하는 것이다.

ACKNOWLEDGMENTS

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (No.2011-0029927).

REFERENCES

[1] M. Tan and X. Su, Media Cloud: When Media Revolution Meets Rise of Cloud Computing, Proc. of The 6th IEEE International Symposium Service Oriented System Engineering(SOSE2011), pp. 251-261, 2011.

[2] W. Zhu et al., Multimedia Cloud Computing, IEEE SIGNAL PROCESSING MAGAZINE. pp. 59-69, 2011.

[3] http://www.icloud.com/

[4] http://www.amazon.com/gp/feature.html/refcd_nav_lm?ie=UTF8&docId=1000796931

[5] http://www.google.com/intl/ko/drive/

[6] http://www.uvvu.com/

[7] Microsoft, Microsoft PlayReady Content Access Technology, White Paper, 2008.

[8] http://www.marlin-community.com/

[9] http://www.openmobilealliance.org/

[10] H. Lee, C, Heo, C, Seo, and S. U. Shin, Design and Implementation of DRM Proxy for DRM Cloud, KIPS Trans. on Comp. and Comm. Sys, Vol. 2, No. 9, pp. 553-560, 2012.

[11] H. Lee, C. Seo, and S. U, Shin, DRM Cloud Architecture and Service Scenario for Content Protection, Journal of Internet Services and Information Security, Vol. 3, No 3, pp. 94-105, 2013.

[12] N. Papanikolaou, S. Pearson, M. C. Mont, and R. Ko, A Toolkit for Automating Compliance in Cloud Computing Services, International Journal of Cloud Computing, Vol. 3, No. 1, pp. 46-68, 2014.

[13] R. Accorsi, A secure log architecture to support remote auditing, Mathematical and Computer Modelling, Vol. 57, pp. 1578-1791, 2013.

[14] A. Gehani, G. F. Ciocarlie, and N. Shankar, Accountable Clouds, 2013 IEEE International Conference on Technologies for Homeland Securith(HST), pp. 403-407, 2013.

[15] J. Yao, S. Chen, and C. Wang, Accountability as a Service for the Cloud, 2010 IEEE International Conference on Services Computing, pp. 81-88, 2010.

[16] R. K. L. Ko, Data Accountability in Cloud Systems, Security, Privacy and Trust in Cloud Systems, pp. 211-238, Springer-Verlag, 2014.

[17] R. K. L. Ko et al. TrustCloud: A Framework for Accountability and Trust in Cloud Computing, 2011 IEEE World Congress on Services, pp. 584-588, 2011.

[18] O. Q. Zhan, M. Krichberg, R. K L Ko, and B. S. Lee, How to Track Your Data: The case for Cloud Computing Provenance, 2011 IEEE International Conference on Cloud Computing Technology and Science, pp. 446-453, 2011.

[19] O. Q. Zhang, R. K L Ko, M. Kirchberg, C. H. Suen, P. Jagadpramana, B. S. Lee, How to Track Your Data: Rule-Based Data Provenance Tracing Algorithms, 2012 IEEE 2011 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, pp. 1429-1437, 2012.

[20] R. K. L. Ko, P. Jagadpramana, and B. S. Lee, Flogger: A File-centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments, 2011 IEEE 10th International Conference of on Trust, Security and Privacy in Computing and Communications(TrustCom), pp. 765-771, 2011.

[21]http://www.highcloudsecurity.comresources/white-papers

[22] S. Pearson et al., Accountability for Cloud and Other Future Internet Services, IEEE 5th International Conference on Cloud Computing Technology and Science, pp. 629-632, 2012.
[23] http://www.a4cloud.eu/

이 혜 주(Lee, Hyejoo)

- 1990년 2월 : 부경대학교 전자계산학과(학사)
- 1997년 2월 : 부경대학교 전자계산학과(석사)
- 2000년 2월 : 부경대학교 전자계산학과(박사)
- 2000년 6월 ~ 2001년 2월: 한국정보통신대학교 박사후 연구과정생
- 2001년 3월 ~ 2005년 1월 : 한국전자통신연구원 디지털방송연구단 선임연구원
- 2005년 3월 ~ 2006년 2월 : 경성대학교 컴퓨터정보학부 초빙교수
- 2006년 3월 ~ 2013년 8월 : 부경대학교 시간강사
- 2013년 7월 ~ 2014년 7월 : 공주대학교 박사후 연구원
- 2014년 8월 ~ 현재 : 숭실대학교 박사후 연구원
- 관심분야 : 디지털 저작권 관리, 멀티미디어 보안, 클라우드 컴퓨팅
- E-Mail : hyejoo2010@gmail.com

서 창 호(Seo, Changho)

- 1990년 2월 : 고려대학교 수학과 졸업(학사)
- 1992년 2월 : 고려대학교 수학과(석사)
- 1996년 8월 : 고려대학교 수학과(박사)
- 1996년 8월 ~ 2000년 2월 : 한국전자통신연구원 선임연구원, 팀장
- 2000년 3월 ~ 현재 : 공주대학교 응용수학과 교수
- 관심분야 : 암호 알고리즘, PKI, 무선 인터넷 보안 등
- E-Mail : chseo@kongju.ac.kr

신 상 욱(Shin, Sang Uk)

- 1995년 2월 : 부경대학교 전자계산학과(학사)
- 1997년 2월 : 부경대학교 전자계산학과(석사)
- 2000년 2월 : 부경대학교 전자계산학과(박사)
- 2000년 4월 ~ 2003년 8월 : 한국전자통신연구원 선임연구원
- 2003년 9월 ~ 현재 : 부경대학교 IT융합응용공학과 교수
- 관심분야 : 암호 프로토콜, 모바일 네트워크 보안, 디지털 포렌식, E-Discovery
- E-Mail : shinsu@pknu.ac.kr