KIPS Tr. Comp. and Comm. Sys.
Vol.2, No.12 pp.553~560 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.12.553

Design and Implementation of DRM Proxy for DRM Cloud Service

Hyejoo Lee† · Changsoo Heo†† · Changho Seo††† · Sang Uk Shin††††

ABSTRACT

The development of cloud computing technology and smart devices have increasingly been expanding the influence in various fields. Although DRM(Digital Rights Management) is a very important technology for secure content services, interoperability among DRM technologies must be addressed in order to provide the service without the constraints of time and place on various smart devices. In this paper, we study DRM Cloud which provides DRM functions as a service in cloud computing environment, and address interoperability problem by providing different DRM technologies as a cloud service. That is, when a user wants to play contents with the different DRM technologies on a smart device, the usage of the content is controlled by providing the corresponding DRM module and function as SaaS from DRM cloud. To do this, we define the functions and structure of DRM Proxy which performs smooth service call and provision between DRM cloud user and DRM cloud, and finally we describe the experimental implementation result.

Keywords : Digital Rights Management(DRM), Cloud Computing, Interoperability

DRM 클라우드 서비스를 위한 DRM Proxy 설계 및 구현

이 혜 주† · 허 창 수†† · 서 창 호††† · 신 상 욱††††

요 약

클라우드 컴퓨팅 기술과 스마트 장치 기술의 발전은 다양한 분야에서 그 영향력을 확대하고 있다. 콘텐츠 서비스에 있어서 콘텐츠를 안전하게 보호하기 위한 DRM(digital rights management) 기술은 매우 중요한 요소로 다양한 스마트 장치에서 시간 및 장소의 제약 없이 서비스를 제공하기 위해서는 DRM 기술 간의 상호 운용성(interoperability)을 해결해야 한다. 본 논문에서는 클라우드 환경에서 DRM 기능들을 서비스로 제공하는 DRM 클라우드를 연구하여 서로 다른 DRM 기술들을 서비스로 제공함으로써 상호 운용성을 해결하고자 한다. 즉, 서로 다른 DRM이 적용된 콘텐츠를 스마트 장치에서 사용하고자 할 때 DRM 클라우드로부터 해당 DRM 모듈과 기능들을 SaaS와 같은 서비스로 콘텐츠의 사용을 제어한다. 이를 위해 DRM 클라우드 사용자와 DRM 클라우드 간의 원활한 서비스 호출과 제공을 수행하는 중개자인 DRM Proxy의 기능과 구조를 정의하고 구현 결과를 기술한다.

키워드 : 저작권 관리 기술(DRM), 클라우드 컴퓨팅, 상호 운용성

1. 서 론

클라우드 컴퓨팅 기술은 IT 환경에 커다란 변혁을 일으키면서 다양한 분야에 적용되기 위해 많은 연구가 이루어 지고 있다[1-2]. 콘텐츠 서비스 분야에도 클라우드 환경에서 다양한 장치를 이용하여 언제, 어디서든지 소비자들이 원한 콘텐츠를 제공하고자 노력하고 있다[3-7]. 콘텐츠 서비스에서 중요한 이슈의 하나로서 콘텐츠 보호 기술인 DRM(digital rights management) 기술은 다양한 스마트 장치에서 콘텐츠를 이용하기 위해서는 서로 다른 DRM 기술 간 상호 운용성(interoperability)을 필요로 한다[8-12]. 상호 운용성은 서로 다른 DRM 기술이 적용된 콘텐츠일지라도 사용자의 장치들에서 이용 가능해야 함을 의미한다. 이러한 목적을 달성하기 위해 지금까지 다양한 노력이 이루어져 왔으나 아직까지 주도적인 기술은 없는 상황이다[13-25]. 클라우드 기술의 영향력이 점차 확대되어 감에 따라 기존의 IT 기능들은 클라우드 환경을 이용하는 서비스 개념으로 변화되고 있다. 그 예로 IDaaS(identity as a service), CaaS(compliance as a service), DSaaS(data storage as a service) 등을 들 수 있다[1]. 이것은 DRM 기술도 포함될 수 있으며, 이에 우리는 클라우드 환경에서 DRM 기능들을 서비스로 제공하는 DRMaaS(DRM as a service), 즉 DRM 클라우드에 관하여

※ 이 논문은 부경대학교 자율창의학술연구비(2013년:CD20130471)에 의하여 연구되었음.
† 정 회 원 : 공주대학교 응용수학과 Post Doc.
†† 비 회 원 : 부경대학교 정보보호협동과정 석사과정
††† 정 회 원 : 공주대학교 응용수학과 교수
†††† 정 회 원 : 부경대학교 IT융합응용공학과 교수
논문접수 : 2013년 10월 11일
심사완료 : 2013년 11월 11일
* Corresponding Author : Sang Uk Shin(shinsu@pknu.ac.kr)

개념과 구조, DRM 클라우드를 이용한 콘텐츠 다운로드, 도메인 관리 서비스 시나리오의 예시 등을 제안하였다[26-27]. DRM 클라우드는 콘텐츠 서비스 제공자들에게 DRM 시스템 구축의 비용과 노력을 없애고 DRM 개발자에게는 DRM 개발을 위한 인프라와 플랫폼을 제공하여 개발 비용의 절감 시키고자 한다. 또 다른 목적으로 클라우드 환경에서 서로 다른 DRM 기술들을 서비스로 제공함으로써 상호 운용성을 해결하고자 한다. 즉, 서로 다른 DRM이 적용된 콘텐츠를 스마트 장치에서 사용하고자 할 때 DRM 클라우드로부터 해당 DRM 모듈과 기능들을 SaaS(software as a service)와 같은 서비스로 제공받아서 콘텐츠의 사용을 제어한다. 이를 위해 DRM 클라우드 사용자와 DRM 클라우드 간의 원활한 서비스 호출과 제공을 수행하는 중개자가 필요하며 이러한 역할을 수행하는 엔티티를 DRM Proxy이라고 한다. 문헌 [28]에서는 DRM Proxy에 대한 구조와 기능에 대하여 간단하게 제안하였으나, 본 논문에서는 좀 더 체계적인 분석을 통하여 DRM Proxy의 기능과 구조를 분류하고 이를 기반으로 설계 및 구현을 논의하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 제2장에서는 현재 제안되어 있는 DRM 기술들에 대해 간단하게 기술한다. 그리고 3장에서는 DRM 기능을 서비스로 제공하는 DRM 클라우드 서비스 모델의 개념에 대하여 설명하고 서비스 제공을 위한 중개자의 역할을 수행하는 DRM Proxy의 기능 및 구조에 대하여 기술한다. 4장에서는 제안한 DRM Proxy의 구현 결과에 대하여 기술하고, 5장에서는 마지막으로 향후 연구과제에 대하여 논의한다.

2. 관련 기술

현재 콘텐츠 보호를 위한 대표적인 기술로 DECE(digital entertainment ecosystem)의 UltraViolet[13-14], MDC(Marlin Developer Community)의 Marlin DRM[15], Microsoft의 PlayReady ecosystem[16-18]과 OMA(open mobile alliance)의 DRM[19-20] 등을 들 수 있다. 이러한 기술들은 기본적으로 다양한 서비스 환경에서 안전하게 콘텐츠를 제공할 수 있는 DRM 기술 개발을 목표로 한다. 이들 기술에 대한 보다 자세한 내용은 참고 문헌들을 참조하길 바라며 이 장에서는 상호 운용성에 대해 고려하고자 한다.

DRM 기술들 간의 상호 운용성의 필요성은 점차 다양한 콘텐츠 서비스가 도입되면서 단일 플랫폼과 단일 기종만을 지원하는 DRM 기술들은 한계에 도달하게 되었다. 이러한 문제로 인해 많은 콘텐츠 사용자들이 DRM이 적용된 콘텐츠의 이용을 외면하는 현상을 초래하게 되었다. 이에 이종의 플랫폼과 기종을 지원할 수 있는 DRM 기술 개발을 위한 여러 가지 연구들이 제안되어 왔다. 먼저, R. Koenen 외는 상호 운용성에 대하여 Table 1과 같이 3가지 접근방법으로 분류하였다[8].

이 분류법을 기반으로 E. Diehl은 Table 2와 같이 5개의 범위로 다시 상호 운용성을 제공하는 방법을 분류하였다[9].

Table 1. Interoperability approaches classified by R. Koenen

분류	특징
Full Format 상호 운용성	콘텐츠, 스마트 장치 등 모두 동일한 형식의 DRM 기술이 적용되는 방식
Connected 상호 운용성	다른 DRM 기술이 적용되면 온라인으로 연결된 시스템에 의해 변환이 되는 방식
Configuration-driven 상호 운용성	시스템 환경에 적절한 툴이 요구 시에 실시간으로 다운로드되거나 설정되는 방식

Table 2. Interoperability approaches classified by E.Diehl

분류	특징
Vertical 상호 운용성	하나의 통합된 포맷과 보호 기법을 사용하여 상호운용성을 지원하는 방법으로 Koenen의 full-format 방식과 동일
Horizontal 상호 운용성	공통의 인터페이스와 메커니즘을 정의하여 상호운용성을 해결하는 방법
Plug-in 상호 운용성	DRM을 실행하는데 필요한 툴을 검색하고 다운로드할 수 있는 프레임워크를 정의하여 상호운용성을 지원하는 방법으로 Configuration-drive 방법과 동일
Translation 상호 운용성	콘텐츠에 적용된 DRM 기술이 서로 다를 때 다른 DRM 기술로 변환하는 방법으로 Connected 방법과 동일
IRL(interoperable rights locker)	Horizontal과 Translation 방법의 혼합으로 공통의 인터페이스와 메커니즘을 이용하면서 사용권한의 변환을 적용하여 상호운용성을 지원하는 방법

이러한 분류법을 통하여 DRM 기술들을 체계적으로 분류하여 상호 운용성에 대한 문제점이나 해결책들을 분석하고자 하였다.

상호 운용성과 관련된 다른 연구 중 G. L. Heileman과 P. A. Jamkhedkar은 DRM 구조를 계층화된 프레임워크(layered framework) 측면에서 분석하였다[10-11]. 이 접근법은 DRM 서버와 DRM 클라이언트 각각에 요구되는 DRM 기능들을 레이어별로 분류하고, 각 레이어 간의 인터페이스를 규격화하여 상호 운용성을 제공하는 개념이었다. 즉 DRM 개발자들이 자유롭게 DRM 기능들을 구현하는 대신에 해당 레이어 간의 인터페이스 규격을 준수한다면 서로 다른 DRM 기술이라고 하더라도 상호 운용성을 제공할 수 있음을 제안하였다.

상호 운용성을 위한 단체들의 노력도 지속적으로 이루어지고 있다. 먼저 Intertrust 사를 필두로 상호 운용성을 위한 오픈 프레임워크 규격을 목적으로 한 Coral[23], Microsoft 사의 PIFF(portable interoperable file format)의 규정[17], 주요 영화사가 포함된 DECE의 UltraViolet[14], 월트 디즈니 사의 KeyChest[24], IDP(interoperable DRM Platform) 개발을 목적으로 하는 DMP(Digital Media Project)[25] 등등 활동이 완료되었거나 현재까지도 활동 중인 경우도 있다. Coral의 상호 운용성 프레임워크는 콘텐츠 사용권한에 대한 변환(translation) 기법을 기반으로 상호 운용성을 지원한다. 즉, 사용권한을 표시한 권한 토큰(rights token)을 이용하여 서로 다른 DRM들이 자신만의 라이선스로 변환하게 된다. Coral은 2012년에 해체되었으며, 이후 DECE의 UltraViolet

의 기반이 되었다. Microsoft사는 AES 128비트 CTR 또는 CBC 모드를 이용하여 암호화된 콘텐츠의 콘테이너로써 PIFF(portable interoperable file format) 파일 포맷을 규정하였다. PIFF는 ISO 14496 베이스 미디어 파일포맷(base media file format)을 기반으로 특정 보호 시스템 헤더 박스(Protection System-Specific Header box), 트랙 암호화 박스(track encryption box), 그리고 선택적 샘플 암호화 박스(optional sample encryption box) 등을 PIFF 파일 포맷의 헤더 정보로 사용한다. 그리고, 공통 암호화 표준(common encryption standard, CENC)과 콘텐츠 복호화 모듈(content decryption module, CDM)을 이용함으로써 PIFF을 지원하는 미디어 플레이어에서 DRM이 적용된 콘텐츠를 자유롭게 이용할 수 있게 된다. UltraViolet은 앞에서 기술했듯이 Coral의 많은 부분을 계승하고 있다. 권한 토큰, 권한 락커(rights locker), 계정(account) 등의 개념을 이용하여 사용자, 사용자 그룹, 도메인들을 연관시켜 권한 락커(rights locker)에서 이를 관리하도록 한다. 특히 UltraViolet은 계정(account)를 이용하여 권한 토큰(rights token)을 권한 락커에 저장하여 관리하게 된다. 이러한 역할을 코디네이터(Coordinator)라는 엔티티가 수행하도록 하였다. Coral이나 UltraViolet 방식들은 IRL 방식에 속한다. 월트 디즈니사가 제안한 KeyChest 방식도 IRL 방식으로 KeyChest DRL(digital rights locker)에 구매정보의 기록, 콘텐츠에 대한 자격증명(entitlement)의 인증(authentication) 등을 요청하여 서로 다른 DRM 간의 상호 운용성을 지원하게 된다. DMP의 특징은 DRM 툴들을 다운로드하는 것으로 표준화된 IDP 하에서 공통의 인증과 등록 기관을 이용하여 허가된 DRM 툴들을 다운로드 하고 실행함으로써 서로 다른 DRM 기술 간의 상호 운용성을 지원한다.

3. DRM Proxy의 설계

3.1 DRM 클라우드 서비스 모델

콘텐츠 보호를 위한 DRM 기능들을 클라우드 환경에서 서비스로 제공하는 것을 DRM-as-a-Service라 하고 이를 DRM 클라우드라고 한다. Fig. 1은 DRM 클라우드 서비스 모델을 나타낸 것으로 DRM 클라우드의 사용자는 콘텐츠 사용자가 소유한 스마트 장치(smart devices), 콘텐츠 소유자와 미디어 클라우드, 그리고 DRM 개발자로 나누어진다. 클라우드 컴퓨팅의 서비스 배치 모델(service deployment model)에 따라 DRM 클라우드 서비스는 3개의 서비스 모델로 나눌 수 있다. DRM 클라우드 서비스를 제공하기 위해 필요한 메모리, 컴퓨팅 파워, 스토리지 등 컴퓨팅 자원을 제공하는 IaaS(infrastructure as a service)를 기반으로 DRM 개발자들에게 DRM 서비스 및 컴포넌트들을 개발하기 위한 개발 환경을 제공하는 PaaS(platform as a service)와 DRM 서비스의 사용자들에게 DRM 모듈 및 서비스를 브라우저와 같은 간단한 사용자 인터페이스 어플리케이션(user interface application, UIA)로 제공하는 SaaS(software as a service) 형태가 가능하다. 이 때 DRM 클라우드와 클라우드 사용자 간의 원활한 서비스 제공을 위해 중계자가 요구된다. Fig. 1에 나타난 바와 같이 이러한 중개자를 DRM 클라우드 환경에서 DRM Proxy라고 한다. 즉, 클라우드 사용자의 요청에 따라 DRM 클라우드 서비스의 요청과 호출을 수행하고 수행되는 서비스를 클라우스 사용자에게 제공한다. 또한 DRM 클라우드 서비스를 관리한다. 특히 DRM 클라우드의 경계에 위치하여 이를 edge-DRM Proxy라 한다.

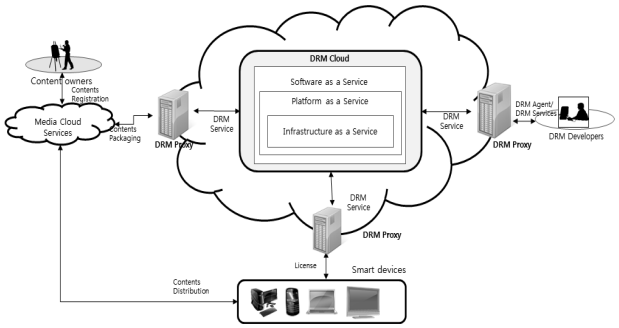

Fig. 1. DRM Cloud service model

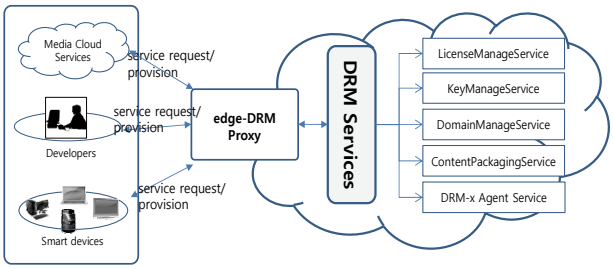

Fig. 2. Role of edge-DRM Proxy within DRM Cloud

DRM 기능은 일반적으로 라이선스 관리 기능, 키 관리 기능, 콘텐츠 패키징 기능, 도메인 관리 기능 등으로 분류될 수 있다. 실제 이러한 기능들이 DRM 클라우드의 서비스로 제공된다. DRM 개발자들은 이러한 기능들을 DRM 클라우드의 PaaS를 이용하여 새로운 서비스를 개발함으로서 콘텐츠 소유자와 미디어 클라우드, 콘텐츠 사용자의 스마트 장치에 새로운 DRM 서비스를 제공할 수 있다. Fig. 2는 이러한 DRM 클라우드 서비스를 제공하기 위한 edge-DRM Proxy의 역할에 대하여 나타내고 있다. 그림에 나타난 바와 같이 미디어 클라우드, 개발자, 그리고 스마트 장치가 edge-DRM Proxy에게 DRM 서비스를 요청하면 edge-DRM Proxy는 요청된 해당 서비스를 DRM 클라우드로 부터 호출한다. 이때 요청된 서비스는 그림에 나타난 바와 같이 라이선스 관리 서비스, 키 관리 서비스, 도메인 관리 서비스, 콘텐츠 패키징 서비스, 그리고 DRM-x Agent 서비스 등이 가능하다. 여기서 DRM-x[1] Agent 서비스는 DRM 클라우드 사용자에게 SaaS로 제공되는 사용자 인터페이스 어플리케이션(UIA, user interface application)을 의미하는데 특히 스마트 장치의 서비스 제공을 위해 필요한 UIA를 DRM Agent라고 한다. DRM Agent는 DRM 제어 모듈로

1) DRM-x에서 x는 클라우드 사용자에게 서로 다른 UIA가 제공됨을 의미함.

정당한 콘텐츠 사용을 허용하기 위한 권한 실행(rights enforcement) 모듈로 스마트 장치에서의 콘텐츠 사용을 위한 모든 동작은 DRM Agent의 제어 하에 있어야 한다. 이와 같은 역할을 수행하는 edge-DRM Proxy의 상세한 기능과 구조에 대하여 아래에 기술한다.

3.2 edge-DRM Proxy 기능

앞에서 기술한 대로 edge-DRM Proxy는 클라우드 사용자의 요청에 따른 DRM 클라우드 서비스의 요청 및 호출, DRM 클라우드 서비스를 실질적으로 클라우드 사용자에게 제공한다. 또한 DRM 클라우드 서비스를 위한 관리 기능들도 요구된다. edge-DRM Proxy에 대한 상세한 기능을 정의하기 위해 먼저 각 클라우드 사용자들로부터의 가능한 서비스 요청에 대해 분석한다.

1) 콘텐츠 이용자(스마트 장치)

콘텐츠 이용자는 자신이 소유한 스마트 장치를 이용하여 콘텐츠를 재생한다. 이때 콘텐츠를 재생하기 위해 스마트 디바이스는 DRM 클라우드로부터 Table 3과 같은 서비스를 요청한다.

Table 3. DRM Cloud services for smart devices

서비스 요청	내용
도메인 생성 및 등록 서비스	안전하게 콘텐츠를 공유하고 사용하기 위한 도메인 생성과 등록 서비스를 요청
스마트 장치 등록	콘텐츠 사용을 위하여 정당한 스마트 장치임을 인가 받기 위해 스마트 장치의 등록 서비스를 요청
스마트 장치의 도메인 가입	생성된 도메인 내 콘텐츠 공유를 위해 생성된 도메인 내에 스마트 장치 가입을 요청
DRM Agent의 실행	콘텐츠 재생 시 적용된 DRM 제어를 위한 DRM Agent의 요청
라이선스 발급 요청	콘텐츠를 재생하기 위해 라이선스가 필요한 경우 라이선스 발급 요청
지속적 사용권한의 관리	지속적인(persistent) 사용권한 관리를 위한 다양한 서비스 요청 예) 재생 횟수 제어에 의한 사용권한 시 재생횟수에 대한 저장 요청

2) 콘텐츠 소유자와 미디어 클라우드

콘텐츠의 소유자는 콘텐츠 관리 및 배포 서비스를 제공하는 미디어 클라우드에 소유권을 가지고 있는 콘텐츠를 등록한다. 실제 콘텐츠 소유자는 미디어 클라우드에 콘텐츠를 등록하기 때문에 DRM 클라우드에 직접 연결하지 않는다. 하지만 콘텐츠 소유자는 콘텐츠 등록시에 DRM 기술에 관한 정보들을 미디어 클라우드로부터 제공받아 자신의 콘텐츠를 배포하는데 적합한 서비스 제공자를 선택해야 한다. 즉 Table 4와 같이 미디어 클라우드가 실질적으로 DRM 클라우드에 서비스를 요청한다.

3) DRM 개발자

DRM 기능을 클라우드 환경에서의 서비스로 제공하는 하나의 이점 중에 개발 비용의 절감을 들 수 있다. 즉, DRM

Table 4. DRM Cloud services for Media Cloud

서비스 요청	내용
DRM 기술 정보 요청	미디어 클라우드는 콘텐츠 소유자들에게 DRM 기술에 대한 정보를 제공하기 위해 현재 서비스되고 있는 DRM 기술들에 대한 정보를 DRM 클라우드에게 요청
콘텐츠 패키징 서비스 요청	콘텐츠 소유자로부터 콘텐츠 등록 요청 시 가장 핵심 서비스로 콘텐츠 암호화를 위하여 콘텐츠 패키징 서비스를 요청

개발자는 DRM 서비스를 개발하기 위한 개발 환경을 DRM 클라우드로부터 제공받아 개발하고 이를 DRM 클라우드에 배치시키기 때문에 기술 개발의 비용을 감소시킬 수 있다. 이와 같은 작업을 위하여 DRM 개발자는 Table 5와 같은 서비스를 요청할 수 있다.

Table 5. DRM Cloud services for DRM Developer

서비스 요청	내용
통합 개발 환경 요청	DRM 클라우드에서 제공하는 통합 개발 환경을 이용하여 DRM 서비스를 개발하기 위한 통합 개발 툴을 포함한 개발 환경 요청
테스트 환경의 요청	DRM 개발자가 개발한 DRM 서비스들이 적절하게 동작되는지를 확인하기 위해 가상의 DRM 클라우드 환경을 요청
개발한 DRM 서비스의 배치	개발된 DRM 서비스를 실제의 DRM 클라우드에 배치하기 위해 DRM 서비스에 관한 정보와 개발한 DRM 서비스의 API, 컴포넌트, 또는 객체 등 실질적인 DRM 서비스 등록을 요청

이와 같이 클라우드 사용자가 요구하는 서비스를 DRM 클라우드로부터 제공하기 위하여 edge-DRM Proxy는 사용자와 DRM 클라우드와의 인터페이스를 제공하고 DRM 클라우드로부터 수행된 서비스를 클라우드 사용자들에게 제공하는 기능으로 분류될 수 있다. 이에 edge-DRM Proxy는 인터페이스를 제공하기 위해 사용자별 인터페이스 제공을 위한 정보의 관리, 사용자 인터페이스 어플리케이션의 관리, 그리고 사용자에게 서비스를 제공하기 위한 DRM 클라우드 서비스 정보의 관리, DRM 클라우드 서비스 제공을 위한 서비스 호출 및 관리 등의 상세 기능들을 제공해야 한다. 이러한 기능을 담당하기 위한 edge-DRM Proxy의 추상적 구조를 다음과 같이 분류할 수 있다.

3.3 edge-DRM Proxy 구조

edge-DRM Proxy는 각각 DRM-x Agent Manager, DRM Service Manager, DRM Service Catalog로 구성되며 각 요소들의 기능에 대하여 아래에 기술한다.

1) DRM-x Agent Manager

DRM 클라우드 사용자를 위한 UIA인 DRM-x Agent들을 관리하고 제공하는 기능을 수행한다. DRM 클라우드 사용자가 DRM 클라우드에 연결하면 DRM 클라우드는 사용자에게 적합한 UIA를 서비스한다. 이때 사용자별 제공되는 UIA의 종류는 Table 6 같이 분류된다.

Table 6. Types of DRM-x Agent UIA

종류	내용
DRM-IE Agent	Media Cloud가 DRM 클라우드에게 DRM 기술에 관한 정보를 요청하고 콘텐츠 패키징 서비스 요청 등을 수행하기 위한 메시징 전달과 수신, 그리고 콘텐츠 패키징을 위한 서비스 호출 기능 제공
DRM-IDE Agent	DRM 개발자의 DRM 서비스 개발을 위한 개발 언어 지원, 에디터, 컴파일러, 디버그 등과 같은 통합 개발 환경 지원, 그리고 테스트 환경 지원 등의 기능 제공
DRM-AD Agent	스마트 장치의 도메인 생성, 가입과 탈퇴 등 도메인 내 콘텐츠 공유를 위한 도메인 관리 기능을 위한 메시징 전달 및 수신, 서비스 호출 기능 제공
DRM Agent	스마트 장치에서의 콘텐츠 사용을 제어하기 위하여 라이선스 발급 요청 기능, 라이선스 파싱 및 사용권한 실행(enforcement) 제어, 콘텐츠 복호화 기능, 미디어 플레이어와의 인터페이스 기능 등을 제공

2) DRM Service Catalog

필요한 DRM 서비스를 수행하기 위한 서비스 정보를 제공하고 관리한다. 즉, 클라우드 사용자들이 DRM 클라우드 서비스를 요청하는 경우에 기본적으로 다음과 같은 정보가 필요하다.

- DRM 서비스의 이름: 요청된 DRM 서비스를 구별하기 위한 식별자
- DRM 서비스의 버전: 동일한 DRM 서비스일지라도 업데이트에 따라 호환성(compatibility)을 위한 버전정보
- DRM 서비스의 위치: 요청된 DRM 서비스가 어디에 배치되어 있는가에 대한 위치 정보(URL)
- DRM 서비스의 특징: 요청시 필요한 DRM 서비스의 파라메터, 지원 가능한 스마트 장치와 콘텐츠 서비스 등 DRM 서비스에 대한 여러 가지 정보들

이 외에도 DRM 클라우드 서비스를 위한 필요한 정보들이 있을 수 있다.

3) DRM Service Manager

DRM 서비스를 제공하기 위하여 DRM 서비스의 등록 및 관리 기능을 수행하고 서비스의 호출 및 서비스를 제공한다.

- DRM 서비스의 배치: DRM 개발자들이 개발한 DRM 서비스의 API, 컴포넌트 등을 실제 DRM 클라우드에 등록
- DRM 서비스의 정보: DRM Service Catalog에 DRM 서비스에 필요한 정보를 등록
- DRM 서비스의 업데이트: 개발한 DRM 서비스의 유지와 보수

이 3가지의 모듈은 서로 연관되어 진다. DRM 개발자가 개발한 DRM 서비스와 정보는 DRM Service Manager에 의해 edge-DRM Proxy에 저장된 후, 서비스 호출 시에 요구되는 정보를 제공하기 위해 DRM Service Catalog에 DRM 서비스 정보들이 저장된다. 이를 이용하여 DRM 클라우드 사용자들은 자신이 요청하는 서비스에 대한 이름, 위치, 기타 파라메터 등에 대해 알게 된다. Fig. 3은 이와 같은

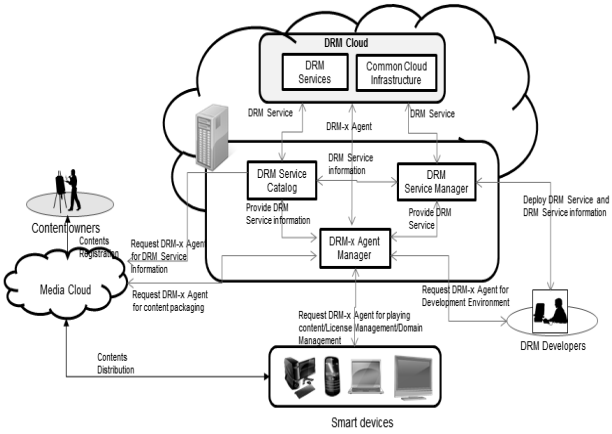

Fig. 3. Structure of edge-DRM Proxy

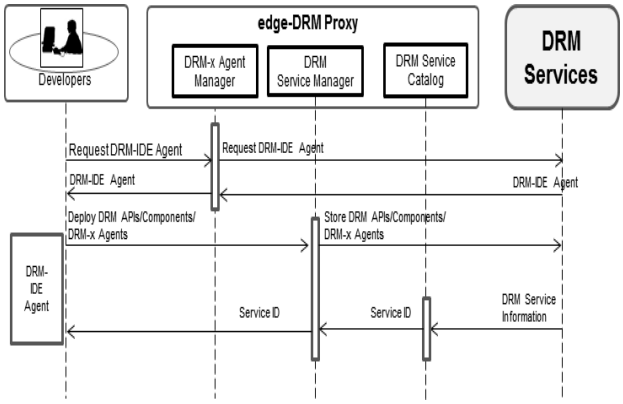

Fig. 4. Work flow of edge-DRM Proxy for DRM Developers

edge-DRM Proxy의 구조를 나타내고 있다. 그림에 나타난 바와 같이 DRM-x Agent Manager는 클라우드 사용자들의 연결 시에 필요한 UIA를 제공한다.

이때 DRM-x Agent Manager는 DRM Cloud로부터 Table 6에 표시한 UIA를 검색하여 이를 SaaS와 같은 형태로 제공하게 된다. 각 사용자별 edge-DRM Proxy의 동작 흐름을 살펴보면 다음과 같다. 먼저, DRM 개발자의 서비스 요청의 경우를 살펴보면 다음과 같다. Fig. 4와 같이 DRM 개발자들이 DRM-x Agent Manager에게 DRM 클라우드의 PaaS 서비스를 위한 UIA, 즉 DRM-IDE Agent를 요청하여 DRM 서비스를 위한 API, 컴포넌트 또는 DRM-x Agent 등을 개발한다. 개발 및 테스트가 완료된 후, 이를 DRM 클라우드에 배치하기 위하여 DRM Service Manager에 요청하면 개발자가 만든 DRM APIs, 컴포넌트 또는 DRM-x Agent를 DRM 클라우드에 등록시키게 된다. 이때 DRM 개발자가 배치시킨 DRM 서비스에 대한 식별자, 버전 등의 정보들이 DRM 클라우드로부터 생성되어 DRM Service Catalog에 저장되고 배치된 DRM 서비스의 식별자는 DRM Service Manager와 개발자에게 전송된다. 서비스 식별자는 클라우드 사용자로부터 DRM 서비스 요청 시 요청되는 서비스를 식별하고 검색하는데 이용된다.

두 번째로 콘텐츠에 대한 패키징을 요청하는 미디어 클라

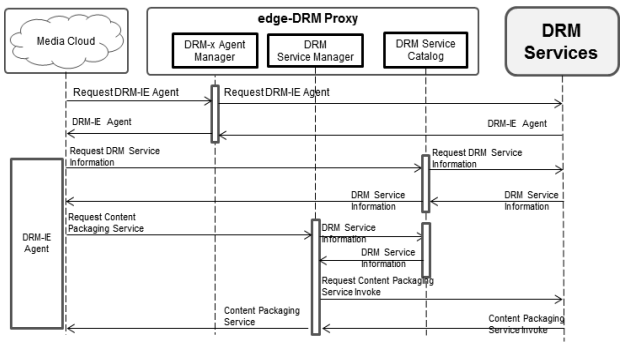

Fig. 5. Work flow of edge-DRM Proxy for Media Cloud

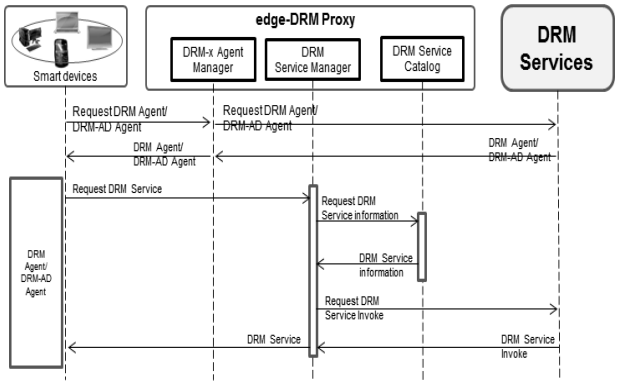

Fig. 6. Work flow of edge-DRM Proxy for smart devices

우드의 서비스 요청은 Fig. 5과 같은 작업흐름을 갖는다. 미디어 클라우드는 DRM-x Agent Manager에 UIA인 DRM-IE Agent를 요청하고 이를 통하여 DRM 클라우드로부터 현재 제공되는 DRM Service에 관한 정보를 제공받는다. 이때 DRM Service에 대한 정보는 DRM Service Catalog에 의해 관리되고 있기 때문에 실질적인 정보는 DRM Service Catalog로부터 제공받게 된다. 이러한 정보로부터 콘텐츠 소유자가 콘텐츠를 패키징 할 DRM 서비스를 선택하면 해당 DRM 기술의 콘텐츠 패키징 서비스를 DRM Service Manager에 요청한다. DRM Service Manager는 DRM 서비스에 대한 보다 상세한 정보 즉 DRM 서비스의 위치, 서비스의 동작 로직 등을 DRM Service Catalog에서 전달 받은 후 그에 따라 DRM Services의 콘텐츠 패키징 서비스를 요청하고 DRM Services는 요청에 따라 서비스를 제공한다.

마지막으로 Fig. 6과 같이 스마트 장치에서는 다양한 서비스 요청이 가능하다. 스마트 장치가 DRM 클라우드 서비스를 요청하기 위해 DRM-x Agent Manager로부터 DRM Agent 또는 DRM-AD Agent를 서비스를 받은 후 DRM Service Manager에게 DRM 서비스를 요청한다. 이때 DRM Service Manager는 요청된 DRM 서비스에 관한 정보(예: DRM 서비스의 위치, 파라메터 등)들을 서비스 식별자를 이용하여 DRM Service Catalog로부터 검색하여 적절한 DRM Service의 실행을 요청한다. DRM 클라우드는 요청된 DRM Service 인스턴스를 실행하고 이를 스마트 장치에게 제공하게 된다.

4. 구 현

이 장에서는 앞에서 기술한 edge-DRM Proxy의 간단한 구현 결과를 기술한다. edge-DRM Proxy의 구현을 위하여 아래와 같은 시스템 환경을 이용하여 테스트 환경을 위한 DRM 클라우드를 구축하였다. 2개의 PC에 각각 CentOS 6.4 64Bit(Intel Core 2quad 2.5GHz, 3Gb RAM), 시트릭스사의 Cloudstack 3.0.2, NFS-Util과 VM(virtual machine)들을 위한 하이퍼바이저로 XenServer 6.0.2(Intel Core2 quad 2.5GHz, 4Gb RAM)를 설치하여 DRM 클라우드 시스템을 구축하고 소켓 통신을 통하여 edge-DRM Proxy가 DRM 서비스를 요청하는 과정을 구현하였다. Fig. 7은 구축한 DRM 클라우드 구조도를 나타내고 있다. 그림에서 나타난바와 같이 XenServer 위에 VM들이 존재하게 되며 이러한 VM들에 DRM 서비스를 위한 어플라이언스(appliance)들이 실행되게 된다.

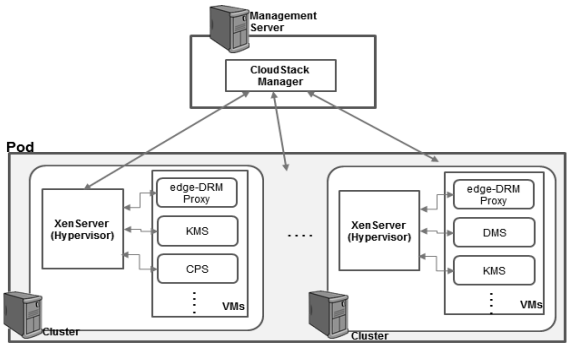

Fig. 7. Structure of DRM Cloud

이와 같이 구축한 DRM Cloud 상에 APM(Apache PHP Mysql)을 이용하여 edge-DRM Proxy의 기능 중 미디어 클라우드로부터 콘텐츠 패키징 서비스 요청을 수행하는 부분을 간단한 형태로 구현하고 그 결과를 다음에 나타낸다. 단, 미디어 클라우드 구현은 제외하였다. 먼저 Fig. 8은 3개의 VM인 (1) 콘텐츠 패키징 서버(CPS, content packaging server), (2) 키 관리 서버(KMS, key management server), (3)edge-DRM Proxy가 실행된 3개의 창을 나타내고 있다.

이때 서로 다른 2개의 DRM 기술인 rootA, rootB를 이용하고 각각 콘텐츠 패키징 서비스를 제공한다고 가정할 때, 다음과 같이 서로 다른 작업 순서로 수행될 수 있다. Fig. 9는 rootA DRM 기술을 이용하여 콘텐츠 패키징 서비스를 수행 한 경우 edge-DRM Proxy에서 먼저 KMS 서비스를 호출하여 키를 생성한 후에 CPS에 연결하여 콘텐츠 암호화를 수행하는 경우의 결과를 나타내고 있다.

이와 달리, rootB 기술은 CPS를 먼저 호출한 후 키 생성을 위해 KMS를 호출하는 작업 순서로 서비스를 수행한다고 가정하면 Fig. 10과 같은 수행 결과를 얻을 수 있다.

이와 같이 동일한 콘텐츠 패키징 서비스라고 할지라도 서로 다른 DRM 기술에 따라 수행 과정이 달라질 수 있다. 그러나 edge-DRM Proxy의 DRM Service Catalog에 의해 이

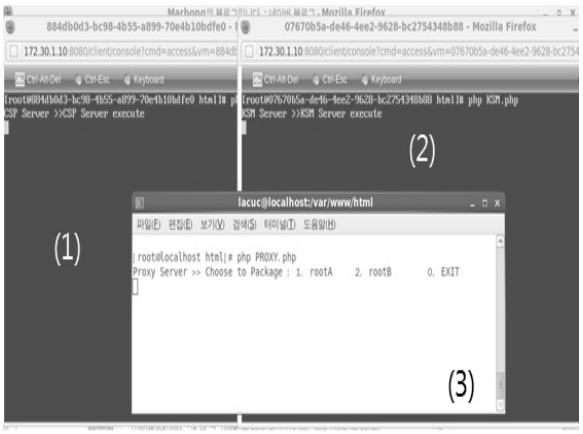

Fig. 8. Implementation of edge-DRM Proxy and DRM Cloud

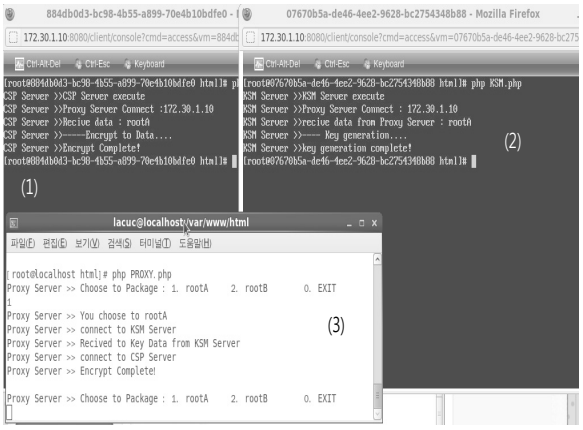

Fig. 9. Implementation results provided by DRM rootA

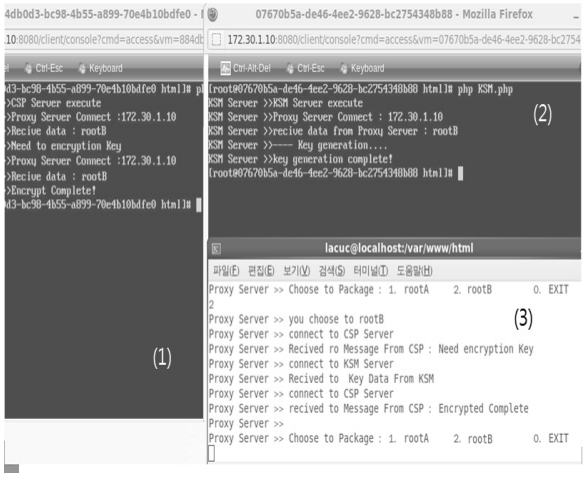

Fig. 10. Implementation results provided by DRM rootB

러한 정보들이 관리되어 있기 때문에 edge-DRM Proxy는 그러한 정보를 기반으로 서로 다른 DRM 기술을 서비스 할 수 있다. 본 구현결과에서는 이러한 정보를 임의로 표현하여 적용하였다. 그러나 이러한 정보들을 표준화된 방법을 이용하여 표현한다면 DRM 기술 간의 상호 운용성 지원에 더욱 효율적일 것이다.

5. 결 론

클라우드 환경은 IT 개발자, 사용자, 그리고 비즈니스 제공자들에게 새로운 IT 환경을 제공함으로써 새로운 서비스 제공을 가능케 하였다. 이와 함께 새롭게 해결해야 할 문제도 안겨 주었다. 클라우드 환경에서의 콘텐츠 서비스는 콘텐츠의 보호를 위한 DRM 기술에 해결해야 할 도전 과제로 상호 운용성을 들 수 있으며 이러한 문제를 해결하기 위한 많은 연구도 이루어지고 있다. 본 논문에서는 클라우드 환경에서 기존의 DRM 기능들을 서비스로 제공하는 DRM 클라우드에 대한 개념을 설명하고 DRM 클라우드 서비스를 위해 DRM 클라우드 사용자와 DRM 클라우드 서비스 간의 인터페이스를 제공하기 위한 중개자로써 DRM Proxy라는 엔티티를 제안하고 실질적인 실현 예로써 edge-DRM Proxy의 기능과 구조, 그리고 구현에 관하여 기술하였다. edge-DRM Proxy의 구현은 2개의 PC를 활용하여 DRM 클라우드 시스템을 구축하고 DRM 클라우드 서비스를 호출하고 실행되는 간단한 구현 결과를 보였다. 향후 연구과제로서 웹 서비스 기술, SOA(service oriented architecture) 등의 개념을 적용하여 DRM 클라우드를 구성하는 엔티티간의 메시지 전달과 서비스 호출을 위한 인터페이스를 정의하고, 구축한 DRM 클라우드 시스템 성능을 향상시키고 다양한 DRM 서비스를 적용하여 상호 운용성을 위한 DRM 클라우드 환경을 구축하고자 한다.

참 고 문 헌

[1] B. Sosinsky, *Cloud Computing*, Wiley Publishing, Inc. 2011.

[2] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy*, O'Reilly Media, 2009.

[3] D. Diaz-Sanchez et. al., "Media Cloud: An Open Cloud Computing Middleware for Content Management," *IEEE Trans. On Consumer Electronics*, Vol.57, No.2, pp.970-978, 2011.

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

[5] W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia Cloud Computing," *IEEE SIGNAL PROCESSING MAGAZINE*, pp.59-69, 2011.

[6] P. Zou, C. Whan, Z. Liu, and D. Bao, " Phosphor: A Cloud based DRM Scheme with Sim Card." *in Proceedings of 12th International Asia-Pacific Web Conference*, Computer Society, pp.459-463, 2010.

[7] R. Petrlic and C. Sorge, "Privacy-Preserving DRM for Cloud Computing," *in Proceedings of 6th International Conference on Advanced Information Networking and Application Workshops*, pp.1286-1291, 2012.

[8] R.H Koenen, J. Lacy, and M. Mackay, and S. Mitchell, "The long march to interoperable digital rights," *in the Proceedings of IEEE*, pp.883-897, 2004.
[9] E. Diehl, *Securing Digital Video Techniques for DRM and Content Protection*, Springer, 2012.
[10] G. L. Heileman and P. A. Jamkhedkar, "DRM Interoperability Analysis from the Perspective of Layered Framework," *in the Proceedings of the fifth ACM workshop on DRM*, pp.17-26, 2005.
[11] P. A. Jamkhedkar and G. L. Heileman, "Digital rights management architecture," *in Computers and Electrical Engineering 35*, pp.376-394, 2009.
[12] T. Kalker, K. Carey, and J. Lacy, "The Coral DRM Interoperability Framework," [Internet] http://www.intertrust.com/download/ccnc07.pdf,2007.
[13] T. Kaler, R. Samtani, and X. Wang, "UltraViolet: Redefining the Movie Industry?," *IEEE Multimedia*, pp.7-11, 2012.
[14] DSystem: System Specification version 1.0.6 [Internet], http://www.uvvuwiki.com/index.php?title=Main_Page.
[15] Marlin broadband architecture overview [Internet], http://www.marlin-community.com/develop/downloads/white_papers.
[16] Microsoft, "Microsoft PlayReady Content Access Technology" [Internet], http://www.microsoft.com/playready/documents/.
[17] J. A. Bocharov, et. al, "Portable encoding of audio-video objects: The Protected Interoperable File Format(PIFF)" [Internet], http://go.microsoft.com/?linkid=9682897.
[18] Microsoft, "Interoperability, Digital Rights Management and the Web [Internet], http://www.microsoft.com/playready/documents/.
[19] open mobile alliance [Internet], http://www.openmobilealliance.org/.
[20] OMA digital rights management v2.0, [Internet] http://technical.openmobilealliance.org/Technical/release_program/drm_v2_0.aspx.
[21] Widevine DRMs [Internet], http://www.widevine.com/wm_drm.html.
[22] Verimatrix MultiRights [Internet], http://www.verimatrix.com/solutions/multirights.php.
[23] Coral Consortium [Internet], http://en.wikipedia/wiki/Coral_Consortium.
[24] KeyChest [Internet], http://en.wikipedia.org/wiki/Keychest
[25] Digital Media Project [Internet], http://www.dmpf.org.
[26] H. Lee. S. Shin, and C. Seo, "Cloud-Based DRM Service 8Model for Secure Contents Service," *The Journal of Digital Policy and Management*, Vol.10, No.10, pp.465-473, 2012.
[27] H. Lee, S. Shin, and C. Seo, "DRM Cloud Architecture and Service Scenario for Content Protection," *Journal of Internet Services and Information Security*, Vol.3, No.3/4, 2013.
[28] H. Lee, W. Shin, and S. Shin, "DRM Proxy of DRM-as-a-Service for Content Protection," *in Proceedings of the 3rd International Conference on Convergence Technology 2013*, pp.287-288, 2013.

이 혜 주

e-mail : hyejoo2010@gmail.com
1990년 부경대학교 전자계산학과(학사)
1997년 부경대학교 전자계산학과(석사)
2000년 부경대학교 전자계산학과(박사)
2000년~2001년 한국정보통신대학교 Post Doc.
2001년~2005년 한국전자통신연구원 디지털방송연구단 선임연구원
2005년~2006년 경성대학교 컴퓨터정보학부 초빙교수
2009년~2013년 부경대학교 시간강사
2013년~현 재 공주대학교 응용수학과 Post Doc.
관심분야 : 디지털 저작권 관리, 멀티미디어 보안, 디지털 워터마킹, 이미지 처리

허 창 수

e-mail : kakadark@naver.com
2013년 동명대학교 정보보호학과(공학사)
2013년~현 재 부경대학교 정보보호협동과정 석사과정
관심분야 : 클라우드 컴퓨팅, 클라우드 컴퓨팅 보안, 암호학

서 창 호

e-mail : chseo@kongju.ac.kr
1990년 고려대학교 수학과(학사)
1992년 고려대학교 수학과(석사)
1996년 고려대학교 수학과(박사)
1996년~1996년 국방과학연구소 선임연구원
1996년~2000년 한국전자통신연구원 선임연구원, 팀장
2000년~현 재 공주대학교 응용수학과 교수
관심분야 : 암호 알고리즘, PKI, 무선 인터넷 보안 등

신 상 욱

e-mail : shinsu@pknu.ac.kr
1995년 부경대학교 전자계산학과(학사)
1997년 부경대학교 전자계산학과(석사)
2000년 부경대학교 전자계산학과(박사)
2000년~2003년 한국전자통신연구원 선임연구원
2003년~현 재 부경대학교 IT융합응용공학과 부교수
관심분야 : 암호 프로토콜, 모바일 네트워크 보안, 디지털 포렌식, E-Discovery