
안전한 콘텐츠 서비스를 위한 클라우드 기반 DRM 서비스 모델

이혜주*, 서창호**, 신상욱***

Cloud-Based DRM Service Model for Secure Contents Service

Hyejoo Lee*, Changho Seo**, Sang Uk Shin***

요 약 모바일 기기와 클라우드 컴퓨팅 기술의 도입은 N 스크린 서비스와 같은 새로운 콘텐츠 서비스를 가능하게 하였다. 새로운 콘텐츠 서비스 환경을 위하여 상호운용성과 다중 플랫폼(multi-platform)을 지원하는 DRM(digital rights management) 기술들이 개발되고 있으나 아직까지 콘텐츠 서비스 가입 변경에 의한 콘텐츠의 이동이나 지원 단말의 구매 등 여러 면에서 사용자에게 불편함을 초래하고 있다. 본 논문에서는 가입 서비스와 상관없이 콘텐츠의 자유로운 이동을 지원하고 사용자가 소유한 다양한 스마트 기기에서 DRM이 적용된 콘텐츠를 자유롭게 사용할 수 있도록 클라우드 컴퓨팅 기반의 DRM 서비스 모델로써 DRMaas(DRM-as-a-Service) 모델을 제안한다.

주제어 : N-스크린 서비스, 저작권 관리 기술, 클라우드 컴퓨팅, 상호운용성

Abstract The mobile devices and cloud computing technology introduced new content services such as N-Screen service. The DRM techniques have been developed to support interoperability and multi-platform for new environment of content service. Nevertheless, it is still inconvenient for the consumers to purchase a new DRM-supported device or to migrate some purchased contents into new device due to the change of the subscription of service. Therefore, in this paper, cloud-based DRM model which is referred as DRMaas (DRM-as-a-Service) model, is proposed to allow the consumer to freely use and move some DRM-protected contents in various smart devices regardless of subscription of service.

Key Words : N-Screen Service, Digital rights management, Cloud computing, Interoperability

1. 서론

최근 스마트 폰과 같은 이동성을 갖춘 모바일 기기와 IT 자원을 필요한 만큼만 서비스하는 클라우드 컴퓨팅 기술[8][9][11][12]이 IT 산업의 화두가 되고 있다. 모바일 기기와 클라우드 컴퓨팅 기술은 시간과 위치에 의한 제약성을 제거함으로써 사용자의 편의성을 증대시키고 IT 자원을 필요로 하는 만큼만 서비스로 제공함으로써 비용을 감소시켜 새로운 서비스 도입에 영향력을 확대시키고

있다. 예로 다양한 스마트 기기 간의 연동과 콘텐츠를 공유하는 새로운 콘텐츠 서비스인 N 스크린 서비스를 들 수 있는데, 이는 다양한 네트워크 환경에서 QoS를 보장함과 동시에 TV, PC, 스마트폰 등 다양한 단말을 소유한 사용자에게 콘텐츠를 서비스한다. 통신사업자, 방송사업자, 단말 제조사 등 각 분야의 업체들은 성공적인 N 스크린 서비스를 위하여 다양한 서비스 전략을 수립하고 있다. <표 1>은 N 스크린 서비스 사업자들의 서비스 전략을 나타내고 있다[1][2].

본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임 (No.2011-0029927).

*부경대학교 IT융합응용공학과

**공주대학교 응용수학과 교수

***부경대학교 IT융합응용공학과 교수(교신저자)

논문접수: 2012년 10월 11일, 1차 수정을 거쳐, 심사완료: 2012년 11월 15일

〈표 1〉 사업자별 서비스 전략

구분	업체	주요 전략
통신사업자	AT&T	하드웨어, 네트워크 서비스 간 통합 지향
방송사업자	컴캐스트, CBS	보유한 방송 콘텐츠의 강점을 바탕으로 TV-PC 연계 강화 및 결합 서비스 전략
인터넷&플랫폼사업자	구글 등	PC에서 보유하고 있는 경쟁력을 바탕으로 모바일과 TV영역 진출 확대
디바이스사업자	애플, 소니, 삼성전자	서비스 플랫폼으로 비즈니스 모델을 확장, 하드웨어와 연계한 서비스 전략

N 스크린 서비스와 같은 디지털 콘텐츠를 서비스하기 위해 고려해야 할 부분은 콘텐츠의 안전한 사용을 위한 DRM(digital rights management) 기술이다. 개별 단말 환경만을 고려해서 개발되었던 DRM 기술들은 N 스크린 서비스 환경에는 적합하지 않고, DRM 기술 간의 상호 운용성(interoperability)을 지원해야 한다. 이러한 인식 의해 다양한 단말들을 지원하는 멀티플랫폼 기반 DRM 기술과 상호 운용성을 제공하고자 하는 DRM 기술들이 제안되었다[3][10][12][15][16][17][18][19][20]. 그러나, 이러한 DRM 기술의 개발에도 불구하고 DRM이 적용된 콘텐츠를 사용하는 데 있어서 콘텐츠 서비스 간에 자유로운 이동이 힘들고, 가입된 서비스를 지원하는 단말 만을 구매해야 하기 때문에 사용자의 입장에서는 불편함을 느끼게 된다. 이에 애플을 비롯한 업체들은 사용자들의 불편함을 해소하기 위해 DRM-free 콘텐츠를 스트리밍 서비스와 같은 제한적인 서비스에 제공하고 있다[13]. 또한, DRM 개발업자나 단말 제조업자는 제공되는 콘텐츠 서비스를 지원하기 위한 적절한 DRM 클라이언트 모듈을 만들어야 하기 때문에 개발 비용의 증가를 초래한다. 따라서, 콘텐츠 서비스 간에 자유로운 이동을 허용하고 사용자가 소유한 다양한 스마트 기기에서도 DRM이 적용된 콘텐츠를 사용할 수 있도록 클라우드 컴퓨팅 개념을 도입한 DRM-as-a-Service(이하 DRMaas) 모델을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 2절에서는 최근 연구되고 있는 DRM 기술을 간략하게 소개한다. 그리고 3절에서는 본 논문에서 제안하는 DRMaas 모델의 개념적인 구조에 대해서 설명하고, DRMaas 모델을 기반으로 콘텐츠 등록, 다운로드 및 이동 등의 콘텐츠 서비스

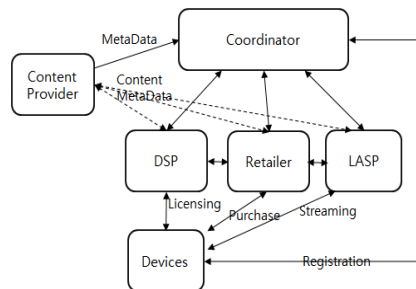
절차에 대해서 기술한다. 4절에서는 제안한 DRMaas 모델과 2절에서 기술한 DRM 기술과의 비교 분석을 통하여 제안하는 DRMaas 모델에 대한 유효성을 고찰한다. 마지막으로 5절에서는 향후 연구과제에 대해 논의한다.

2. 관련 DRM 기술

디지털 기술의 발전에 의해 콘텐츠의 무분별한 불법 복제에 대처하기 위하여 DRM 기술들이 지속적으로 연구되고 있다. 초기에는 단순히 암호화에 의한 콘텐츠 접근 제어를 수행하였으나 다양한 서비스 시나리오 적용을 위해 콘텐츠 공유, 이동 등 장치 및 도메인 관리 기술들이 추가되고 있다. 이에 본 절에서는 현재 대표적인 DRM 기술에 대해 간략하게 소개한다. 각 DRM 기술에 대한 세부적인 내용은 참고문헌을 참고하기 바란다.

2.1 UltraViolet 에코시스템

6개의 메이저 영화제작사와 70개 이상의 회원업체로 이루어진 컨소시엄에 의해 DECE(digital entertainment content ecosystem)인 UltraViolet 에코시스템을 개발하였다[18]. UltraViolet은 클라우드 기반의 디지털 권한 인증 기술을 이용하여 사용자의 단말간 콘텐츠 공유기능을 지원하는데 코디네이터(coordinator)라는 개념을 이용하여 사용권한을 제어하고 관리한다. 또한 도메인 개념을 가족 멤버 간에 적용하여 멤버 간의 콘텐츠 공유를 허용하고 있다. [그림 1]은 UltraViolet에코 시스템의 구조를 나타내고 있다.

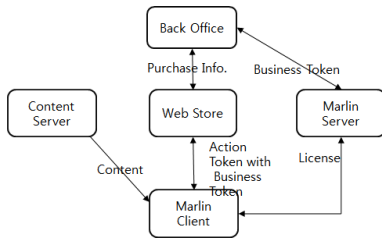


〔그림 1〕 UltraViolet 에코 시스템

2.2 Marlin DRM

Marlin DRM은 개방형 DRM 플랫폼으로 intertrust, Panasonic, PHILIPS, Samsung, Sony의 5개사로 이루

어진 MDC(Marlin Developer Community)에 의해 개발되어 상업적 성공을 위한 상호운용성과 개방성을 목표로 한다[16]. [그림 2]에 나타난 바와 같이 Marlin Client와 Marlin Server는 클라이언트가 처리해야 할 명령들을 포함한 액션토큰(Action Token)과 비즈니스 로직에 따른 절차들을 포함하는 비즈니스 토큰(Business Token)들을 이용하여 다양한 스마트 기기들에 콘텐츠를 제공한다.



[그림 2] Marlin DRM 구조

Marlin Client는 SDK로써 라이선스를 요청하고 도메인 가입, 그리고 콘텐츠에 대한 접근을 제어하여 콘텐츠 사용을 허용한다. Marlin 시스템은 노드(node)와 링크(link)의 개념을 이용하여 도메인을 관리한다. 예를 들면 PMP를 소유한 사용자 “철수”가 영화 “도둑들”을 구매하였다고 한다면 PMP, 철수, 영화를 노드로 표시하고 각 노드 간에 링크를 연결함으로써 도메인을 구성하게 된다. 이때 사용자 “영희”를 새로운 노드로 추가하는 경우에 영화 “도둑들”에 대하여 사용자 “영희”와 “철수”가 서로 공유할 수 있도록 허용되어 진다.

2.3 MS PlayReady

마이크로소프트는 1999년에 Window Media DRM(WMDRM)을 개발하여 다양한 분야에서 이용되어왔다[15]. 이후 마이크로소프트는 환경 변화에 따라 다양한 서버들로 구성되는 PlayReady 서버와 PlayReady 클라이언트로 구성되는 PlayReady 에코시스템이라고 하는 새로운 DRM 기술을 개발하게 되었다. PlayReady는 스트리밍과 프로그래시브 다운로드를 지원하는 온라인 서비스와 1회성 구매, 대여, 가입 기반의 오프라인 서비스를 설정하여 다양한 시나리오에서 콘텐츠 보호를 위한 기술을 지원한다. PlayReady DRM 기반의 콘텐츠 서비스 과정을 살펴보면 사용자가 유통서버에 저장된 DRM-protected 콘텐츠를 재생하려고 하는 경우 클라이언트는 콘텐츠와 헤더를 다운로드하게 된다. 콘텐츠를 다운로드

한 후에 콘텐츠를 복호하기 전에 사용자 컴퓨터에 IBX(individualized black box)라는 적절한 DRM 소프트웨어가 설치되어 있지 않으면 IS(individual server)로부터 이를 다운로드하여 설치해야 한다. 이후에는 라이선스 획득과 도메인 등록 등을 수행하여 콘텐츠를 재생하게 된다.

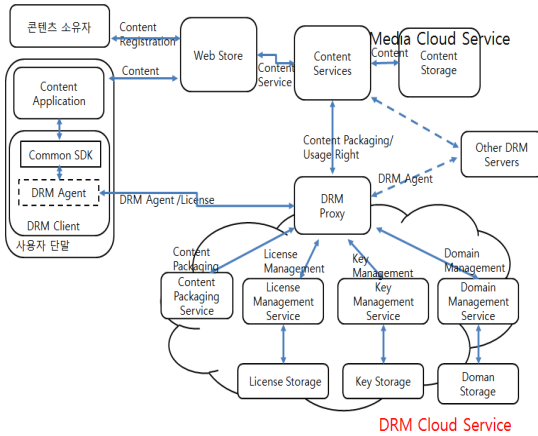
2.4 국내 DRM 현황

국내 DRM 기술은 음악, 동영상, 전자책 등 콘텐츠 유통 서비스와 회사 내 문서 보안 등에 적용되고 있다. 이와 같이 다양한 분야에서 이용되고 있는 국내 DRM 기술들은 DRM 업체들이 자체적으로 개발한 기술을 적용하고 있기 때문에 상호호환성과 관련한 문제들이 존재하고 있다. 이에 따라 TTA 등 CAS와 DRM 간 상호연동을 위한 인터페이스, EXMI 등 상호연동을 위한 인터페이스를 위한 표준화 활동[5][6][7]과 DRM 기술 발전을 위한 국내 DRM 업체들이 한국DRM업체협의회를 설립하였다. 하지만 업체 간 이해관계로 인하여 상호호환이 가능한 DRM이 적용된 제품이나 서비스가 제공되지 않는 것이 현실이다. 또한 UltraViolet 서비스와 같은 클라우드 기반의 콘텐츠 유통을 위한 클라우드 DRM은 국내에서 서비스되거나 개발되고 있는 사례는 매우 적다[4]. 하지만 클라우드 환경 하에서 콘텐츠 생명주기동안 콘텐츠 보호를 위한 클라우드 DRM에 대한 기술 연구 및 개발이 앞으로 활발하게 이루어질 전망이다.

3. 클라우드 기반 DRM 서비스 모델

기존 DRM 시스템이 콘텐츠 서비스 시스템 내부의 서브시스템으로 제공되는 것과 달리 제안하고자 하는 DRMaaS 모델은 독립 시스템으로 콘텐츠 소유자, 콘텐츠 서비스 제공자, 그리고 사용자에게 콘텐츠에 대한 패키징, 라이선스 생성 및 발급, 키 생성 및 관리에 필요한 자원 및 기능을 온디맨드(on-demand) 서비스로 제공하는 것을 목적으로 한다. [그림 3]은 다양한 스마트 기기에서 콘텐츠를 안전하게 이용하고 사용자의 서비스 이용 시 콘텐츠의 공유, 이동 등 자유로운 사용을 제공하기 위해 DRMaaS 모델의 개념적인 구조를 나타내고 있다. 그림에 나타난 바와 같이 DRMaaS 모델 기반의 콘텐츠 서비스는 성공적인 네트워크 연결을 가정하며 콘텐츠 소유

자, 사용자 단말, Media Cloud Service와 DRM cloud Service로 구성된다. 여기서 DRM Cloud Service가 본 논문에서 다루고자 하는 DRMaas를 제공하는 부분으로 DRM Proxy와 DRM 기능을 제공하는 서비스 부분과 라이선스, 키 등을 저장하는 부분들로 구성된다. 콘텐츠 서비스를 제공하는 Media Cloud Service는 본 논문의 범위를 벗어나는 부분으로 상세하게 다루지 않는다.



[그림 3] DRMaas 모델의 개념적 구조

DRMaas 모델의 주요 엔티티와 기능들을 살펴보면 다음과 같다.

- 콘텐츠 소유자: 콘텐츠에 대한 소유권을 가지고 콘텐츠 서비스 제공자에게 콘텐츠를 배포하기 위해 콘텐츠를 제공한다. 이때 콘텐츠 소유자는 콘텐츠에 대한 정보, 사용정책, 서비스 제공자를 선택한다.
- Web Store: 콘텐츠 등록이나 콘텐츠 구매를 위하여 콘텐츠 소유자와 사용자가 콘텐츠 서비스에 접속할 수 있도록 웹 브라우저 또는 전용 플레이어를 이용한 사용자 인터페이스를 제공한다. 이때 Web Store는 서비스 제공자들의 콘텐츠 서비스 통합 환경을 제공한다.
- Media Cloud Service: 콘텐츠 배포를 담당하는 엔티티로 콘텐츠 다운로드이나 스트리밍 서비스를 제공하고 콘텐츠 등록 및 콘텐츠 구매를 위한 처리를 수행한다.
- 사용자 단말: 사용자가 콘텐츠를 재생하기 위한 단말. 단말은 Content Application, Common SDK, DRM Agent로 구성된다. Content application은 사용자와 상호동작을 위한 인터페이스, 그리고 단말에

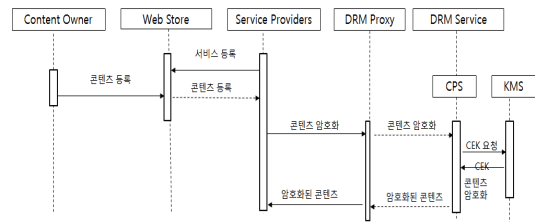
서 DRM Agent의 구동을 위한 Common SDK 호출 기능, 콘텐츠 처리 기능들을 제공한다. Common SDK는 DRM Agent를 단말에서 구동을 위하여 DRM Proxy 간 통신 기능을 제공한다. DRM Agent는 DRM 기능을 제공하는 주요 모듈로써 DRM Proxy로부터 해당 Agent 모듈을 다운로드하여 콘텐츠 접근 제어, 라이선스 관리 등 기능을 수행한다.

- DRM Proxy: 클라우드 기반의 DRM 서비스를 제공하는 주요 엔티티로써, 대리인의 자격으로 DRM 관련된 정보를 관리하고 키 관리, 도메인 관리, 라이선스 관리, 콘텐츠 패키징 등 여러 가지 DRM 서비스를 호출하여 각 엔티티에게 서비스를 제공한다.

DRMaas 모델 기반 콘텐츠 서비스는 다운로드 서비스 시나리오를 고려한다. 따라서 콘텐츠와 라이선스를 다운로드 받아 콘텐츠 이동, 공유 및 재생이 가능하고, 도메인을 구성하여 도메인의 멤버로 등록된 단말에서만 콘텐츠의 사용을 허가한다.

3.1 콘텐츠 서비스 및 콘텐츠 등록

[그림 4]는 콘텐츠 서비스 제공자에 의해 서비스 등록과 콘텐츠 소유자에 의한 콘텐츠 등록 과정을 나타내고 있다.



[그림 4] 콘텐츠 서비스 및 콘텐츠 등록 과정

(1) 서비스 등록

먼저 Media Cloud Service를 이용하는 서비스 제공자들은 Web Store에 콘텐츠 서비스를 위해 자신들의 서비스를 등록한다.

(2) 콘텐츠 등록

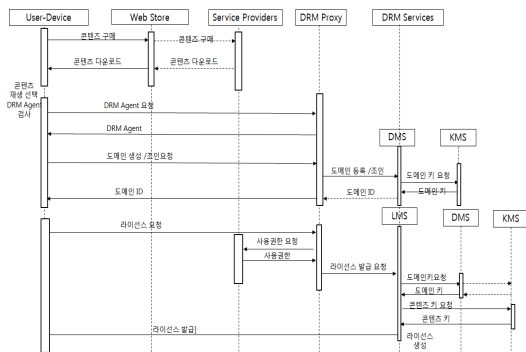
- 콘텐츠 소유자는 자신이 소유한 콘텐츠를 배포할 서비스 제공자를 선택하기 위해 Web Store에 연결하여 서비스 제공자들에 대한 정보를 검색한다. 적

당한 서비스 제공자를 선택하여 사용권한 정보와 함께 콘텐츠를 등록시킨다.

- 웹 스토어를 통해 콘텐츠를 제공받은 서비스 제공자는 DRM Proxy에게 콘텐츠 암호화를 요청한다.
- 요청받은 DRM proxy는 콘텐츠 암호화 키 CEK(content encryption key)를 생성하기 위하여 KMS(key management service)를 호출하고 생성된 CEK를 이용하여 콘텐츠를 암호화하기 위하여 CPS(content package service)를 호출한다. 암호화가 완료되면 서비스 제공자에게 암호화된 콘텐츠를 전송한다.

3.2 콘텐츠 다운로드 및 라이선스 획득

이와 같이 콘텐츠 소유자와 콘텐츠 서비스 제공자들이 콘텐츠 서비스를 시작하면 사용자들은 Web Store를 통하여 콘텐츠를 구매하게 된다. [그림 5]는 콘텐츠 구매 및 라이선스 다운로드 과정을 나타내고 있으며 각 단계의 세부 내용을 아래에 기술한다.



[그림 5] 콘텐츠 다운로드 및 라이선스 획득 과정

(1) 콘텐츠 구매

- Consumer가 콘텐츠를 구매를 위한 Web Store에 접속하여 서비스를 받기 위한 서비스 제공자 및 콘텐츠를 선택하여 콘텐츠를 선택하여 구매 요청을 한다.
- 구매 요청을 받은 Web Store와 서비스 제공자는 구매를 위한 지불 과정을 수행한 후 콘텐츠를 다운로드한다. DRM 서비스 관련 정보 등이 함께 제공되어야 한다.

(2) 콘텐츠 재생

- 사용자 단말에 다운로드된 콘텐츠를 선택하여 콘텐

츠를 재생하면 사용자 단말은 Common SDK를 이용하여 해당 콘텐츠와 관련된 DRM Agent가 존재하는지 확인한다. 적합한 DRM Agent가 없으면 DRM Proxy에 DRM Agent를 요청한다. DRM Proxy가 해당 단말이나 콘텐츠에 적합한 DRM Agent를 검색하여 다운로드하고 단말은 해당 DRM Agent를 구동시키게 된다. 이후 단계에서는 DRM Agent와 DRM Proxy 간에 서로 통신을 수행하게 된다.

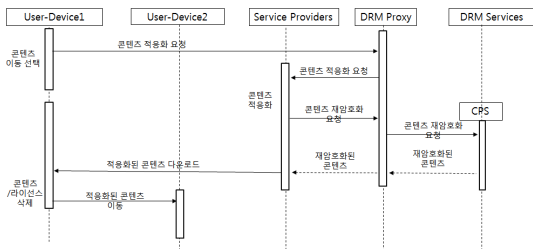
- DRM Agent가 구동된 이후 해당 Device가 Domain에 등록해야 할 필요가 있을 때 DRM Proxy에 요청한다. 이 요청에 따라 DRM Proxy는 해당 DMS(domain management service)를 호출한다.
- DMS는 도메인 생성/가입 요청에 따라 도메인 ID를 생성하고 도메인 키 생성을 위하여 KMS를 호출하여 도메인 키를 생성한다. 도메인 키는 해당 도메인 내에서만 콘텐츠 재생이 가능하도록 라이선스 발급 시 콘텐츠 키를 암호화하기 위해 필요하다.
- 도메인 키를 받은 DMS는 생성된 도메인을 식별하기 위한 도메인 ID를 단말에 전송한다.

(3) 라이선스 발급

- 콘텐츠 재생을 위해 DRM Agent가 DRM Proxy에게 라이선스 획득 요청을 수행한다.
- 요청을 받은 DRM Proxy는 해당 콘텐츠에 대한 사용권한을 서비스 제공자에게 요청한다. 콘텐츠에 대한 사용권한은 서비스 제공자로부터 제공받음으로써 DRM Proxy는 사용권한 정책의 변경에 영향을 받지 않고 라이선스 발급을 수행할 수 있다.
- 사용권한을 기반으로 라이선스를 생성하기 위해 DRM Proxy는 LMS(license management service)를 호출한다. 이때, 라이선스에 콘텐츠 암호화 키, 도메인 키 등이 포함하기 위한 KMS와 DMS를 호출하여야 한다.
- 라이선스의 생성이 완료되면 DRM Proxy는 발급된 라이선스를 사용자 단말에 전송한다.

3.3 콘텐츠 이동

아래의 [그림 6]은 다른 단말로 콘텐츠를 이동(move)시켜 사용하기 위한 과정을 나타내고 있다. 콘텐츠 이동은 라이선스에 이동을 위한 권리가 있을 경우 허용이 된다.



[그림 6] 콘텐츠 이동 과정

(1) 콘텐츠 적응화

- User-Device1은 이동시키고자 하는 콘텐츠를 타켓 단말의 성능에 적합한 콘텐츠의 적응화를 DRM Proxy에게 요청한다.
- DRM Proxy는 콘텐츠에 대한 적응화를 서비스 제공자에게 요청한다.

(2) 콘텐츠의 재암호화

- 콘텐츠 적응화 요청에 따라 적응화를 시킨 콘텐츠에 대하여 서비스 제공자는 DRM Proxy에게 재패키징을 요청한다.
- DRM Proxy는 이 요청에 따라 적응화된 콘텐츠를 재암호화하기 위하여 콘텐츠 패키징 서비스를 호출한다. 이때 콘텐츠 암호화 키는 이전의 암호화 키를 이용한다.

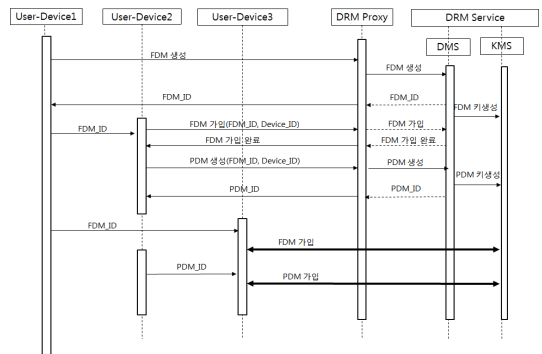
(3) 재암호화된 콘텐츠의 전달

- DRM Proxy는 재암호화된 콘텐츠를 서비스 제공자와 User-Device1에게 전송한다. 이때 적응화되고 재암호화된 콘텐츠를 User-Device2가 네트워크 기능을 소유한 단말인 경우에는 User-Device2에 바로 전송 가능하다.
- User-Device1은 User-Device2인 타겟 단말에 콘텐츠를 전송하고 마지막으로 콘텐츠와 라이선스를 단말에서 삭제한다.
- User-Device2는 전송된 콘텐츠를 사용하기 위해서는 3.2의 콘텐츠 다운로드 및 라이선스 발급 단계 중 (2)콘텐츠 재생, (3)라이선스 발급 단계를 수행한다.

3.4 콘텐츠 공유

콘텐츠 공유는 도메인을 설정하고 해당 도메인에 속한 단말들간에 서로 콘텐츠를 이용할 수 있도록 하는 것을 의미한다. DRMaas 모델의 도메인은 크게 패밀리 도

메인(Family Domain)과 개인 도메인(Personal Domain)으로 분류한다. 일반적으로 홈 내의 모든 장치를 가족 구성원들이 공유하는 환경을 고려하지만 홈 내에서도 특정 장치만을 자신의 도메인으로 설정하여 자신 이외의 구성원에게는 콘텐츠에 대한 접근을 허용하지 않도록 할 수 있다. 이에 패밀리 도메인은 가족 구성원들이 모두 접근할 수 있는 장치들의 그룹을, 개인 도메인은 특정 사용자만 소유한 장치의 그룹을 의미한다. [그림 7]은 장치 User-Device1, User-Device2, User-Device3가 각각 패밀리 도메인의 멤버, User-Device2와 User-Device3는 개인 도메인의 멤버인 경우 도메인 생성, 가입 과정을 나타내고 있다.



[그림 7] DRMaas 모델의 도메인 관리

(1) 도메인 생성

- 패밀리 및 개인 도메인을 관리하는 FDM(family domain manager)와 PDM(personal domain manager)를 생성하기 위해 사용자는 DRM Proxy에게 도메인 생성을 요청한다.
- DRM Proxy는 DMS를 호출하여 FDM과 PDM를 생성하여 각각의 ID를 DRM Proxy를 거쳐 사용자에게 전달한다. 이때 DRM Proxy는 FDM/PDM을 위하여 키 관리 서비스를 호출하여 도메인 키 FDM_K, PDM_K를 생성하도록 한다.

(2) 도메인 가입 및 탈퇴

- 각 장치들이 도메인에 가입하기 위해 DRM Proxy에 FDM_ID, PDM_ID, Device_ID를 전송하면 DRM Proxy는 DMS를 호출한다.
- DMS는 장치 ID와 도메인 ID를 데이터베이스에 저장하여 장치를 도메인에 등록시킨다.

- 만일 장치가 도메인을 탈퇴하고자 하는 경우 DRM Proxy에 FDM_ID와 PDM_ID, Device_ID를 전송하면 DRM Proxy는 DMS를 호출하고 DMS는 데이터베이스에서 Device_ID를 제거하여 장치를 탈퇴시키고 DRM Proxy는 DMS로부터의 응답 결과에 따라 DRM Agent에 FDM_ID나 PDM_ID를 삭제하도록 한다.

(3) 도메인 라이선스 획득

- 설정된 도메인 내에 등록된 장치가 라이선스를 획득하기 위해 DRM Proxy에 라이선스를 요청하는 경우에는 그림5의 라이선스 획득 과정에서 FDM_ID이나 PDM_ID, 그리고 Device_ID를 함께 전송해야 한다.
- DRM Proxy는 전송된 도메인 ID와 Device_ID를 이용하여 DMS에게 등록된 도메인과 단말인지를 확인할 것을 요청한다.
- 확인이 성공하면, CEK와 이를 암호화하기 위한 도메인 키에 대한 정보들을 얻기 위하여 KMS를 호출하여 CEK와 도메인 키를 획득하여 최종적으로 LMS에 전달하여 라이선스 생성을 요청한다.
- 만일 패밀리 도메인 키로 CEK가 암호화된 경우에는 패밀리 도메인 내에 모든 콘텐츠에 대한 접근이 허용될 수 있으나 개인 도메인 키로 암호화된 경우에는 개인 도메인 내 콘텐츠만 접근 가능하게 된다.

4. 비교 분석

본 절에서는 DECE의 UltraViolet, MDC의 Marlin, MS의 PlayReady DRM을 제안한 DRMaaS 모델과의 비교 내용을 기술한다.

UltraViolet 에코시스템과 DRMaaS 모델의 유사점은 클라우드 기반의 DRM 시스템을 제안하고 있다는 것이다. 특히 UltraViolet 에코시스템의 코디네이터와 DRMaaS 모델에서의 DRM Proxy는 도메인 관리, 단말 관리, 권한 관리와 관련한 주요 기능 등을 제공하고 있다. 차이점은 DRMaaS 모델의 DRM Proxy는 서비스에 대한 사용자 계정이나 콘텐츠에 대한 메타데이터, 사용권한에 대한 정보들은 관여하지 않고 그러한 정보들이 필요할 경우에 서비스 제공자에게 요청하여 처리한다. 또한 UltraViolet

에코시스템은 DECE 계정을 기반으로 도메인을 구성하고 있기 때문에 홈 내에서 복수의 도메인(multiple domain)을 지원하지 않고 있다.

Marlin 시스템은 Marlin 서버를 통하여 라이선스 발급 등의 처리를 수행한다. 따라서 Marlin 서버는 DRMaaS의 DRM Proxy와 유사하다. 또한 Marlin 시스템의 단말에 설치된 Marlin Client의 SDK는 DRMaaS 모델의 Common SDK는 어플리케이션과 서버단의 인터페이스 기능을 제공하는 것은 유사하지만, Marlin Client SDK는 Web Store에서 콘텐츠 구매 시 수신한 액션 토큰에 따라 Marlin 서버에 필요한 라이선스 발급 요청 등을 수행한다. 이와 달리 DRMaaS 모델의 Common SDK는 DRM Agent, DRM Proxy, 어플리케이션과의 인터페이스 기능을 제공하는 것으로 단말에서의 DRM 관련된 모든 처리는 DRM Agent에 의해 수행된다.

PlayReady 에코시스템은 클라이언트에 DRM 모듈인 IBX가 존재하지 않으면 다운로드 받아서 설치하는 Downloadable DRM 모듈을 제공한다. 이것은 DRM Agent를 DRM Proxy로부터 다운로드하는 DRMaaS 모델과 유사하나 DRM Proxy와 같이 중앙에서 제어하지 않고 대부분 서버들이 독립적으로 운영되는 차이가 있다.

DRMaaS 모델과 각 시스템 간의 비교 결과를 정리하면 <표 2>와 같이 나타낼 수 있다. 즉, DRMaaS 모델은 클라우드 기반의 UltraViolet의 코디네이터의 기능, PlayReady 에코시스템의 Downloadable DRM 모듈의 기능, 그리고 Marlin 시스템의 SDK 제공에 의한 공통 인터페이스 제공 기능을 모두 포함한다.

<표 2> 각 DRM 시스템과 DRMaaS 모델의 비교

	UltraViolet	Marlin	PlayReady	DRMaaS
중앙제어	○	△	×	○
Downloadable DRM	×	×	○	○
Common SDK	×	○	○	○
Single domain	○	○	○	○
Multiple domain	×	○	×	○

이와 같이 DRMaaS 모델을 기반으로 하는 DRM 시스템은 다음과 같은 이점을 가진다.

- 콘텐츠 소유자는 특정 서비스 제공자에 의존하지 않고 다양한 콘텐츠 서비스를 선택하여 콘텐츠를 배포할 수 있다.
- 콘텐츠 서비스 제공자는 DRM 시스템 구축에 필요

한 비용이 들지 않고, 여러 가지 DRM 서비스를 선택하여 이용하거나 서비스 중에도 변경 가능하다.

- 사용자는 자신의 단말이나 DRM이 적용된 콘텐츠에 적합한 DRM Agent를 다운로드하여 콘텐츠를 사용하기 때문에 특정 콘텐츠 서비스가 제공하는 DRM에 의존하지 않는다. 따라서 가입형 서비스를 제공받는 경우 다른 서비스로 가입을 변경하더라도 다운로드된 콘텐츠는 DRMaaS 시스템에 의해 지속적으로 사용 가능하다.
- DRM 개발자는 라이선스 관리, 패키징 관리 등 여러 가지 관련 기술을 개발할 필요 없이 DRMaaS 시스템에 의해 제공되는 기능을 이용하기 때문에 개발 비용 및 시간을 감축시킬 수 있다.

또한 기존 DRM 시스템과 DRMaaS 시스템의 상호 연동을 고려할 때, 기존 DRM 시스템을 이용할 수 있도록 DRM Agent를 구현하여 DRM Proxy에 등록시켜 둔다면 기존 DRM 시스템을 이용하고 있는 단말장치들은 기존의 DRM 시스템들을 그대로 이용할 수 있을 것이다.

5. 결론

본 논문에서는 N 스크린 서비스와 같은 새로운 콘텐츠 서비스의 도입을 위하여 클라우드 기반 DRM 모델을 제안하고, 기존 DRM 시스템들과의 차이점을 비교하여 각 시스템마다 제공되지 않는 기능들이 제공되고, DRMaaS 모델을 기반으로 기존 DRM 시스템을 그대로 이용할 수 있음을 제시하였다. 지금까지 본 논문에서는 DRMaaS 모델의 개념적인 구조를 제안한 것으로, 앞으로 DRMaaS 모델의 엔티티 간 프로토콜 및 데이터 정의, 그리고 서비스 구축 시에 요구되는 기술적 요구사항, 네트워크 성능, 서버의 성능, 단말의 성능에 대한 분석과 기존 DRM 방식과의 상호 연동 방안 등에 대하여 지속적인 연구가 요구된다.

참고 문헌

[1] 김윤화 (2010). N 스크린 전략 및 추진 동향 분석. 방송통신정책. 22(20). 1-23.
 [2] 문혜란, 김신호, 정병호 (2010). 콘텐츠 공유기술 동향

분석. 전자통신동향분석. 25(4). 112-120.

[3] 이승민, 권혁찬, 서동일 (2012). 스마트 미디어 시대의 콘텐츠 보호 기술 동향. 주간기술동향. 11-21.
 [4] 오성훈 (2012). 클라우드 보안과 저작권 보호 기술 동향. 저작권동향 제17호. 한국저작권위원회.
 [5] TTAS.KO-08.0020 (2008). Export/Import(EXIM)를 이용한 디지털 콘텐츠의 DRM 상호 연동 인터페이스. 한국정보통신기술협회.
 [6] TTAS.KO-12.009/R1 (2010). CAS와 DRM 간의 상호연동을 위한 인터페이스. 한국정보통신기술협회.
 [7] TTAS.KO-12.0163 (2010). 패킷 스트림 단계에서의 DRM 상호 연동 인터페이스. 한국정보통신기술협회.
 [8] D. Diaz-Sanchez et. Al. (2011). Media Cloud: An Open Cloud Computing Middleware for Content Management. IEEE Trans. On Consumer Electronics, 57(2). 970-978.
 [9] M. Tan, X. Su (2011). Media Cloud: When Media Revolution Meets Rise of Cloud Computing. Proc. of The 6th IEEE International Symposium Service Oriented System Engineering(SOSE2011). 251-261.
 [10] Microsoft (2008). Microsoft PlayReady Content Access Technology. White Paper.
 [11] P. Zou, C. Whan, Z. Liu, D. Bao (2010). Phosphor: A Cloud based DRM Scheme with Sim Card. Proc. of 12th International Asia-Pacific Web Conference. Computer Society. 459-463.
 [12] T. Kaler, R. Samtani, X. Wang (2012). UltraViolet: Redefining the Movie Industry?. IEEE Multimedia. 7-11.
 [13] W. Zhu, C. Luo, J. Wang, S. Li. (2011). Multimedia Cloud Computing. IEEE SIGNAL PROCESSING MAGAZINE. 59-69.
 [14] www.apple.com/pr/library/2007/04/02Apple-Unveils-Higher-Quality-DRM-Free-Music-on-the-iTunes-Store.html
 [15] msdn.microsoft.com/en-us/library/cc838192(v=vs.95).aspx
 [16] www.marlin-community.com/
 [17] www.verimatrix.com/solutions/multirights.php
 [18] www.uvvu.com/
 [19] www.openmobilealliance.org/
 [20] www.widevine.com/drm.html

이혜주



- 1990년 2월 : 부경대학교 전자계산학과 (학사)
- 1997년 2월 : 부경대학교 전자계산학과 (석사)
- 2000년 2월 : 부경대학교 전자계산학과 (박사)
- 2000년 6월 ~ 2001년 2월 : 한국정

보통신대학교 박사후 연구과정생

- 2001년 3월 ~ 2005년 1월 : 한국전자통신연구원 디지털방송연구단 선임연구원
- 2005년 3월 ~ 2006년 2월 : 경성대학교 컴퓨터정보학부 초빙교수
- 2009년 3월 ~ 현재 : 부경대학교 시간강사
- 관심분야 : 디지털 저작권 관리, 멀티미디어 보안, DRM, 디지털 워터마킹
- E-Mail : iamhj@paran.com

서창호



- 1990년 : 고려대학교 수학과 졸업 (학사)
- 1992년 : 고려대학교 수학과 (석사)
- 1996년 : 고려대학교 수학과 (박사)
- 1996년 ~ 1996년 : 국방과학연구소 선임연구원
- 1996년 ~ 2000년 : 한국전자통신연

구원 선임연구원, 팀장

- 2000년 ~ 현재 : 공주대학교 응용수학과 교수
- 관심분야 : 암호 알고리즘, PKI, 무선 인터넷 보안 등
- E-Mail : chseo@kongju.ac.kr

신상욱



- 1995년 2월 : 부경대학교 전자계산학과 (학사)
- 1997년 2월 : 부경대학교 전자계산학과 (석사)
- 2000년 2월 : 부경대학교 전자계산학과 (박사)
- 2000년 4월 ~ 2003년 8월 : 한국전

자통신연구원 선임연구원

- 2003년 9월 ~ 현재 : 부경대학교 IT융합응용공학과 부교수
- 관심분야 : 암호 프로토콜, 모바일 네트워크 보안, 디지털 포렌식, E-Discovery
- E-Mail : shinsu@pknu.ac.kr