CI-DRM: 클라우드 기반의 상호운용이 가능한 DRM 시스템*

이훈정, 은하수, 오희국
한양대학교 컴퓨터공학과
e-mail:hoonjung@hanynag.ac.kr

CI-DRM: Cloud based Interoperable DRM System*

Hoonjung Lee, Hasoo Eun, Heekuck Oh
Dept. of Computer Science and Engineering, Hanyang University

요 약

DRM(Digital Right Management)은 디지털 콘텐츠의 사용을 제어하고, 불법복제 및 유통을 방지하는 기술 및 서비스이다. 인터넷의 발달로 디지털 콘텐츠의 불법사용, 불법복제, 불법유통 등이 지속적으로 증가하는 상황에서 DRM의 중요성은 점점 더 커지고 있다. 현재의 DRM 시장은 다수의 DRM 시스템이 혼재하고 있는 상황으로 서로 다른 DRM 시스템간의 상호운용과 표준화에 대한 요구가 커지고 있고 이 문제에 관한 많은 연구가 진행되고 있다. 본 논문에서는 클라우드 컴퓨팅 환경 기반의 서로 다른 DRM 시스템 간 상호운용이 가능한 시스템을 제안한다. 제안하는 시스템은 클라우드 컴퓨팅 서비스 모델 중 SaaS(Software as a Service)를 기반으로 설계 하였으며 현재 사용되고 있는 DRM 시스템 쉽게 적용할 수 있는 장점을 가진다.

1. 서론

현재의 인터넷은 넓은 서비스 범위아 빠른 속도를 자랑한다. 하지만 더 넓은 서비스 범위와 더 빠른 네트워크 속도를 위한 연구가 지속적으로 이루어지고 있다. 이러한 네트워크 환경의 출현으로 최근에는 스마트폰, 테블릿 PC와 같은 네트워크에 연결할 수 있는 기기들의 종류와 수가 폭발적으로 증가하였다. 사용자들은 이러한 기기들을 음악, 동영상등과 같은 멀티미디어 콘텐츠의 이용을 위해 주로 사용한다. 이러한 환경을 바탕으로 멀티미디어 콘텐츠에 대한 사용자들이 수요가 크게 증가하고 있는 실정이다. 멀티미디어 콘텐츠의 수요가 증가함에 따라 이를 불법으로 사용, 복사, 배포하는 행위 또한 크게 증가하고 있다.

디지털 콘텐츠를 불법으로 사용, 복사, 배포하는 행위는 콘텐츠 제작자의 수익과 직결되기 때문에 매우 민감하고 중요한 문제라 할 수 있다. 현재 온/오프라인 상에서 유통되고 있는 대부분의 멀티미디어 콘텐츠는 DRM (Digital Right Management) 이라는 기술을 사용하여 콘텐츠 제작자의 저작권을 보호하고 있다. 저작권 보호에 대한 중요성이 커짐에 따라 DRM의 중요성도 함께 증가할 것이다. DRM은 등장 초기부터 여러 업체에서 자신들만의 기술을 가지고 시장을 형성해왔다. DRM은 콘텐츠를 보호하는 기술이기 때문에 기술이 가지는 안전성을 최우선으로 한다. 이러한 기술적 특성 때문에 DRM 업체들은 자사의 보호 기술 공개를 꺼려하고 있다. 업체들 마다 다른 기술을 사용하기 때문에 다수의 DRM이 시장에 혼재하게 되었고 현재까지도 이런 상황이 계속 유지되고 있다. 현재처럼 한명의 사용자가 스마트폰, 테블릿 PC, MP3 플레이어 등 다수의 기기를 사용하는 OPMD (One Person Multi Device) 환경을 위해서는 현재의 DRM은 표준화와 DRM간 상호운용에 대한 문제를 해결해야 한다. DRM의 표준화와 DRM간 상호운용에 관한 연구는 현재까지도 활발히 진행되고 있다.

본 논문에서는 DRM간 상호운용을 위해 클라우드 컴퓨팅 환경을 이용하였다. 제안하는 시스템은 클라우드 컴퓨팅 모델 중 소프트웨어 및 관련 데이터는 중앙에 호스팅되고 사용자는 클라이언트를 통해 접속하는 형태의 소프트웨어 전달 모델인 SaaS (Software as a Service)를 기반으로 설계하였다. 우리의 기법은 DRM간 효율적인 상호운용이 가능하며 기존 DRM 시스템의 큰 변경 없이 적용가능 하다는 장점을 가진다.

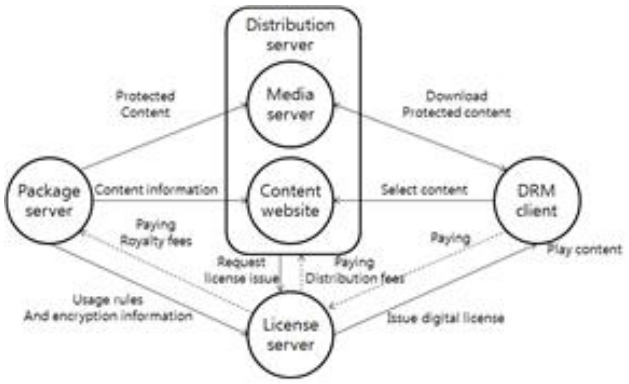
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2012-H0301-12-4004)

* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-R1A2A2A01046986)

2. 배경지식

2.1 DRM과 상호운용

DRM은 콘텐츠 보호와 관련된 총체적 기술이다[1]. 그러나 DRM의 가장 일반적인 기능은 콘텐츠를 암호화하고, 암호화에 사용된 키를 라이센스에 포함시켜 권한이 있는 사용자만이 콘텐츠를 이용할 수 있도록 하는 것이다. 그림 1은 일반적인 DRM 시스템의 구성과 동작을 나타낸다. Package server는 콘텐츠를 CEK (Contents Encryption Key)를 이용해 암호화 하며, License server



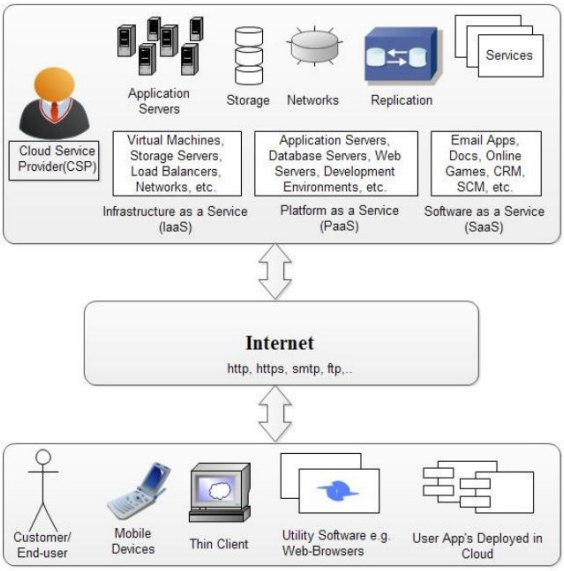
(그림 1) DRM 시스템의 구성과 동작

는 CEK를 디바이스의 공개키로 암호화하여 라이센스를 생성한다. 암호화된 콘텐츠와 이에 해당하는 라이센스를 획득한 DRM client는 라이센스를 복호화하여 CEK를 얻고 CEK를 이용해 콘텐츠를 복호화하여 재생할 수 있게 된다. 이러한 환경에서 콘텐츠를 복호화 하는데 사용되는 CEK와 디바이스의 개인키는 안전하게 관리되어야 하며 사용자 또한 이를 획득할 수 없어야 한다.

DRM 시스템은 등장 초기부터 여러 업체에서 자신들만의 기술을 가지고 시장을 형성해왔기 때문에 제각기 다른 환경과 다른 시스템 혼재하고 있다. 사용자가 소유하는 단말의 수가 증가하는 환경에서 DRM간 상호운용은 매우 중요한 문제가 되었다. 예를 들어 A라는 DRM 시스템으로 보호되고 있는 콘텐츠는 A DRM 시스템이 탑재되어 있는 기기에서만 사용이 가능하며 다른 DRM 시스템을 탑재되어 있는 기기에서는 사용할 수 없게 된다. 사용자들이 사용하는 단말들이 동일한 DRM 시스템을 사용하지 않는 이상 구매한 유료 콘텐츠를 여러 기기에서 사용하는 것이 불가능하다. 이런 문제를 해결하기 위해 DRM의 표준화와 DRM간 상호운용에 대한 연구가 활발히 진행되고 있다.

2.2 클라우드 컴퓨팅

클라우드 컴퓨팅은 인터넷 기술을 이용하여 가상화된 IT 자원을 서비스로 제공하는 컴퓨팅을 의미하는데 기존의 인터넷 기반 컴퓨팅에 비하여 비즈니스 모델이 단순하고 활용 가능성이 높아 IT 업계에 많은 변화를 가져올 것으로 예상되는 기술이다[2]. 클라우드 컴퓨팅의 가장 대표적인 서비스 모델은 소프트웨어를 서비스로 제공하



(그림 2) 클라우드 컴퓨팅 구조

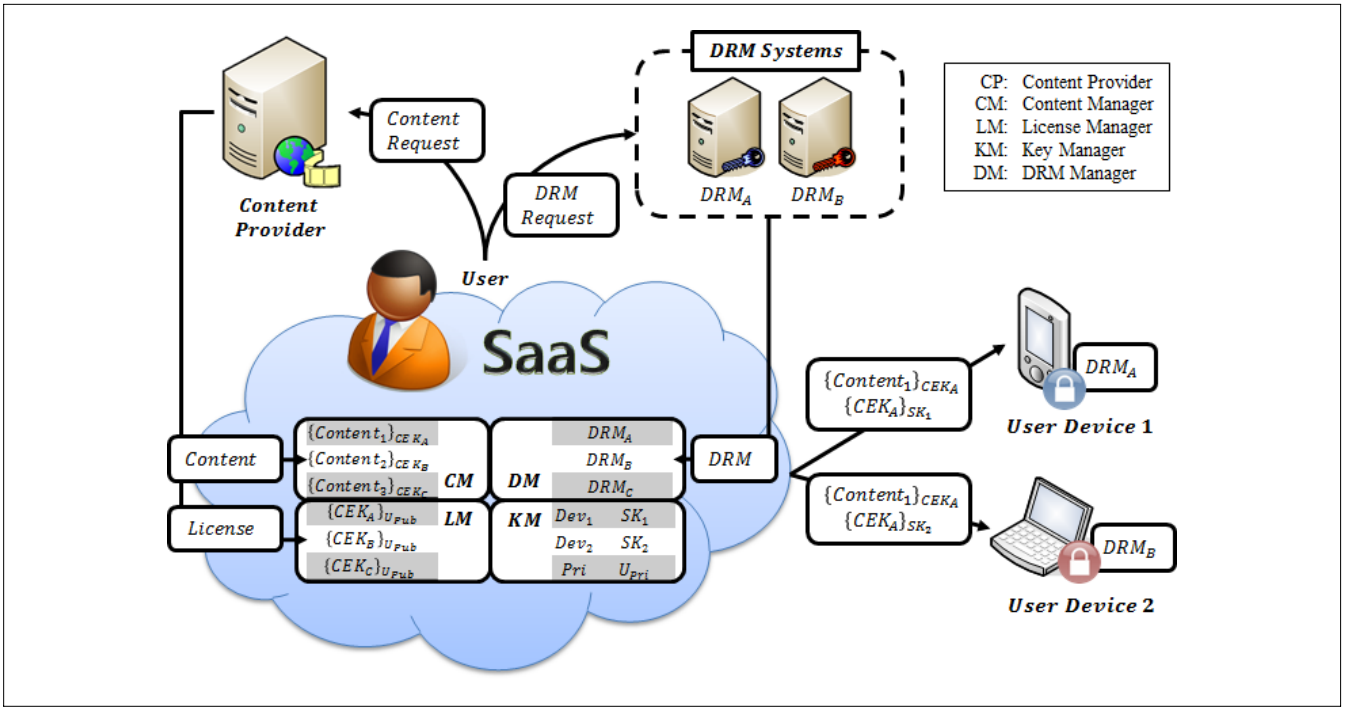
는 SaaS (Software as a Service), 소프트웨어 개발 환경인 플랫폼을 서비스로 제공하는 PaaS (Platform as a Service) 그리고 컴퓨팅 시스템을 서비스로 제공하는 IaaS (Infrastructure as a Service)이다. 그림 2는 일반적인 클라우드 컴퓨팅의 구조를 보여준다[3].

클라우드 컴퓨팅이 보다 활성화되고 널리 사용되기 위해 해결해야 할 문제 중 가장 중요하게 문제는 보안이다. 여러 보안 문제 중에서도 클라우드에 저장되는 사용자들의 데이터에 대한 기밀성과 무결성 보장이 가장 중요한 문제이다. 클라우드 사업자(운영자)의 사용자 정보 오남용을 방지하기 위해서는 법, 제도와 같은 정책적인 부분도 중요하지만 사용자의 데이터 노출과 위변조를 막기 위한 기술적인 부분도 중요하다.

3. 클라우드 기반 상호운용이 가능한 DRM 시스템

3.1 DRM 시스템간 상호운용성

서로 다른 DRM 시스템간 상호운용에 대한 연구는 MPEG-21[4], OMA (Open Mobile Alliance)[5], DMP (Digital Media Project)[6], Coral[7] 등 여러 단체에서 지속적으로 이루어지고 있다. 2010년 V. Rodrigues는 DRM 시스템간 상호운용을 위한 기법을 Full format, Connected, Configuration-driven 3가지로 분류하였는데 첫 번째로 Full format 방식은 DRM 업체들이 합의된 형태로 라이센스를 만드는 방식인데 이는 표준화가 전제되지 않는 한 실현되기 어려운 방식이라 할 수 있다. 두 번째 Connected 방식은 온라인상에서 사용하고자 하는 DRM 시스템의 라이센스 형태로 변경하는 방법인데 이를 위해 DRM 업체들은 자사가 사용하는 라이센스의 구조를 공개하고 기기들이 항상 온라인에 있어야 가능한 방법인데 이는 최근 인터넷 환경을 고려한다면 기기들이 온라인상에 있어야 한다는 점은 크게 무리가 되지 않지만



(그림 3) CI-DRM의 구조와 동작

DRM 업체들이 구조를 공개하는 것을 꺼려하기 때문에 실현되기 힘들다는 문제가 있다. 마지막으로 Configuration-driven 방식은 사용하고자 하는 DRM 시스템 소프트웨어를 인터넷을 통해 다운로드 하거나 기기의 저장 공간에 저장하고 있는 방식인데 이 방법은 기기의 하드웨어와 연동되는 시스템을 사용하는 시스템에서는 사용이 제한된다는 단점을 가지고 있다[8].

DRM 시스템간 상호운용을 위해 가장 중요한 부분은 라이센스로부터 콘텐츠를 복호화하는데 필요한 CEK를 얻어 내는 과정이다. 이는 결국 사용자 인증 방법, 암호화에 사용된 키들의 생성과 전달 및 관리 방법이 DRM 시스템 간 상호운용의 핵심임을 의미한다.

3.2 제안하는 시스템

제안하는 시스템은 3.1절에서 설명한 DRM 간 상호운용을 위한 기법 중 Configuration-driven 방식과 클라우드 컴퓨팅의 서비스 모델 중 SaaS 그리고 공개키 암호기법을 기반으로 한다.

그림 3은 제안하는 시스템의 구조와 동작과정을 보여준다. 제안하는 시스템은 사용자와 사용자의 단말, 콘텐츠를 제공하는 콘텐츠 제공자 그리고 클라우드로 구성된다. 클라우드에는 DRM 시스템을 관리하는 DM (DRM Manager), 콘텐츠를 관리하는 CM (Contents Manager), 라이센스를 관리하는 LM (Licence Manager) 그리고 사용자의 콘텐츠를 암/복호화하는데 사용되는 키들을 관리하는 KM (Key Manager)가 소프트웨어 형태로 존재하며 시스템은 다음의 순서로 동작한다.

① 기기등록: 사용자는 자신의 개인키와 기기들을 클라우드에 등록한다. 이때 클라우드와 기기간에는 비밀키를 공유하게 되며 이러한 키들은 클라우드내의 KM에서 관리한다. (각각의 기기는 서로 다른 각각의 DRM 시스템을 사용한다.)

② 콘텐츠 구매 및 라이센스 획득: 사용자는 각각의 단말에서 자유롭게 콘텐츠를 구매할 수 있으며 콘텐츠 구매 시 그에 해당하는 라이센스를 발급 받는다. 이때 콘텐츠와 라이센스는 기기와 클라우드에 모두 저장할 수 있다.

③ CEK의 획득 및 재생: 각각의 기기들은 기기에 내장되어 있는 각각의 DRM 시스템을 사용하여 라이센스에 포함되어 있는 사용자의 공개키로 암호화되어 있는 CEK인 $\{CEK_{U_{pub}}\}$로부터 CEK를 획득하여 콘텐츠를 재생할 수 있다.

④ 상호운용을 위한 재암호화: 기기에 내장되어 있지 않은 DRM으로 보호되어 있는 콘텐츠를 재생하기 위해서는 먼저 클라우드에서 DRM 시스템에 DRM 클라이언트를 요청하여 다운로드받아 설치한 후, DRM 클라이언트를 이용하여 CEK를 획득한다. 그런 다음 재생하고자 하는 기기에 CEK를 전달한다. CEK를 전달할 때는 CEK의 노출을 막기 위해 기기등록 단계에서 생성된 SK를 이용해 암호화하여 전달한다. (DES나 AES같은 대칭키 암호기법을 사용한다.)

⑤ CEK 전달 및 재생: 4번에서 전달받은 $\{CEK\}_{SK}$를 복호화하여 CEK를 획득한 후 콘텐츠를 재생할 수 있다.

4. 분석

기존 DRM 상호운용을 위한 Configuration - driven 방식이 가지고 있던 기기의 하드웨어와 연동되는 시스템을 사용하는 시스템에서는 사용이 제한된다는 단점을 클라우드 컴퓨팅의 SaaS 모델을 이용하여 극복하였다. 사용자의 기기에 DRM 클리이언트를 다운받는 것이 아니라 클라우드 내에 다운받고 그것을 이용하여 CEK를 획득하고 이를 기기에 전달하는 방식으로 설계하였다.

제안하는 시스템이 가지는 장점은 서로 다른 DRM 스시템을 사용하는 여러 종류의 단말에서 DRM의 종류와 상관없이 콘텐츠를 사용하는 것이 가능하고 기존의 DRM 시스템과 환경을 거의 변화시키지 않고 그대로 적용할 수 있다는 점이다.

5. 결론 및 향후과제

본 논문에서는 Configuration-driven 방식의 DRM간 상호운용 기법과 SaaS 클라우드 컴퓨팅 서비스 모델 기반의 서로 다른 DRM간 상호운용이 가능한 DRM 시스템(CI-DRM)을 제안하였다. 제안하는 시스템은 클라우드에서 콘텐츠, 라이센스, 키를 관리하는 방법으로 OPMD (One Person Multi Device) 환경에서 사용자의 사용성과 편의성을 위한 효율적인 DRM 시스템이다. 또한 기존의 DRM 시스템의 큰 변경 없이 적용하는 것이 가능하다는 장점을 가진다.

향후에는 제안하는 시스템이 가지는 효율성과 안전성에 대한 정량적인 분석을 통해 제안하는 시스템이 가지는 장점을 구체적으로 제시할 것이다.

참고문헌

[1] Wikipedia, “Digital Right Management,” http://en.wikipedia.org/Digital_rights_management.

[2] 김명준, “Korea’s Cloud Computing Strategy,” 2009년 IT21 글로벌 컨퍼런스, 2009년 5월.

[3] M. Srinivasan, K. Sarukesi, P. Rodrigues, M. Manoj and P. Revathy, “State-of-the-art Cloud Computing Security Taxonomies - A Classification of Security Challenges in the Present Cloud Computing Environment,” International Conference on Advances in Computing, Communications and Informatics, ICACCI 2012, Aug. 2012.

[4] MPEG-21, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm.

[5] OMA 2.0, http://www.openmobilealliance.org.

[6] DMP, http://www.dmpf.org.

[7] Coral, “Coral Consortium Core Architecture 3.0,” http://www.coral-interop.org.

[8] R. Koenen, J. Lacy, M. Mackay and S. Mitchel, “The Long March to Interoperable Digital Rights Management,” the IEEE, Vol. 92, pp. 883-897, 2004.