Multi-Media 환경에서 DRM 기술과 국내 업계 동향 분석

김헌*

1. 서론

디지털 문화가 빠르게 확산되면서 다양한 디지털 컨텐츠의 개발과 사용이 급격하게 증가하고 있다.

디지털 컨텐츠는 21세기 문화 산업을 이끌어갈 가장 중요한 요소이자 고부가가치를 창출하는 원동력이 되고 있다. 디지털 컨텐츠의 양적인 증가와 더불어 이제는 질적으로 우수한 컨텐츠 개발로 세계시장을 선도해 나가야 하는 중요한 과제를 안고 있다.

이러한 우수한 디지털 컨텐츠를 불법으로 사용하거나 무단으로 도용하는 사례를 원천적으로 차단하고 보호하기 위하여 DRM(digital rights management)이라는 개념이 도입되었다.

DRM에 주요한 목적은 시간과 노력에 산물인 디지털 컨텐츠에 대한 경제적 가치를 보호하고 적법한 사용을 통한 유통과정의 투명성을 확보하여 더 수준 높은 디지털 컨텐츠 문화를 확대 재생산하는데 있다.

DRM 시스템에 관한 정보와 국내에 DRM 업계에 동향에 관해서 살펴본다.

2. DRM 핵심적 요소 기술

DRM(digital rights management)은 다양한 멀티미디어 컨텐츠의 유통에 있어서 저작권을 보호하고 관리할 수 있는 기술이다. 멀티미디어 컨텐츠의 서비스에 대해서는 서비스 주체별로 다양한 정책이 존재하며, 따라서 DRM도 다양한 형태로 존재할 수 있고 서비스에 적용될 수 있다. DRM이 서비스

주체의 정책에 따라서 다양성을 가지고 있으나 저작권 보호 및 유통관리라는 측면에서 핵심적인 요소기술이 존재한다. [5][6]

2.1 DRM 암.복호화 기술

DRM의 핵심적 요소 기술은 컨텐츠의 보호를 위한 암·복호화 기술과 사용규칙 제어기술, 과금결제를 위한 기술의 3가지로 분류해 볼 수 있다.

DRM시스템에서 있어 가장 중요한 기술은 암호화 기술로서 고객의 비밀번호 혹은 고객 컴퓨터의 고유번호를 암호키로 사용하여 컨텐츠를 암호화하여 전달하기 때문에 이를 복사하여 제3자에게 전달하여도 풀리지 않도록 하는 점이 가장 중요하다. 물론 DRM은 이외에도 컨텐츠 사용규칙 제어기술, 과금 결제를 위한 기술 등의 부대적인 기술들이 필요하다.

이중에서 암복호화 기술은 멀티미디어 컨텐츠의 유통에 있어서 불법유통이나 불법복제를 방지하기 위한 핵심 기술로서, 컨텐츠를 특정한 암호 키를 이용하여 암호화시킴으로써 적법한 사용자만이 복호화하여 컨텐츠를 사용할 수 있도록 하는 기술이다. 기존의 컨텐츠 전달시스템은 사용자 ID와 비밀번호만을 사용하고 있는데 이런 경우 ID와 비밀번호를 공유함으로써 쉽게 컨텐츠를 불법으로 사

* 한신대학교 교양전산학과

용할 수 있다는 문제가 있다. 이것을 해결하기 위하여 (1) 고객 컴퓨터의 고유ID를 변형하여 사용하는 방법 (2) 고객의 PKI키나 은닉된 개인 키를 사용하는 방법이 있다.

고객 컴퓨터의 고유번호, 예를 들면 HardDisk 번호 라든가 혹은 CPU번호를 이용하여 컨텐츠를 암호화 시키는 경우가 있지만 컴퓨터의 고유번호는 누구나 쉽게 접근할 수 있기 때문에 보안성이 떨어진다는 단점이 있다. 따라서 가장 일반적인 DRM암호화 방법은 PKI 개인키처럼 개인 비밀키를 컴퓨터에 내장하고 이를 사용하는 방식이다. 고객의 고유키로 암호화할 경우 장점은 다운로드 받은 컨텐츠를 제3자에게 전달하여도 제3자의 컴퓨터에서는 작동이 불가능하다는 점이다. 이 점을 이용하여 DRM시스템은 컨텐츠의 불법 복제와 유통을 방지할 수 있는 것이다.

암・복호화 시스템에서는 다양한 암・복호화 알고리즘이 존재하며, 그 안정성도 널리 알려진 바가 있으므로 사용에 문제는 없으나 암호 키의 관리나 배포 부분에 있어서의 기술적 차이가 있다.[11][12]

2.2 DRM 사용규칙 제어기술

다음으로 사용규칙 제어기술을 들 수 있는데, 사용규칙에 대해서는 서비스 주체의 서비스 정책과 상당히 밀접한 관련이 있다. 사용규칙에는 사용자에게 유통된 컨텐츠의 사용권한 관리가 상당부분을 차지한다. 컨텐츠의 사용에 있어서 그 컨텐츠를 재생하는 것에 대해서 무한정으로 허용할 것인가 아니면 정해진 횟수의 재생만을 허용할 것인가에 대한 부분이나 컨텐츠의 양도에 대해서도 허용여부를 결정하고 관리하는 것이다. 사용규칙 제어기술이 갖추어야 할 대표적인 것은 서비스 주체에 따른 다양한 서비스 정책을 지원할 수 있는 유연성이라 하겠다.

서비스 주체에 따라서는 공익성을 목표로 하기 때문에 다양한 정보를 무료로 제공하는 곳이 있는가 하면 수익성을 목표로 유료 컨텐츠를 제공하는 곳이 있다. 저작권이 있는 컨텐츠의 서비스에는 사용자에게 서비스 사용료를 부과하고 결제할 수 있는 시스템과 저작권의 라이센스에 따른 분배를 수행할 수 있는 기술적 지원이 필요하다. 과금 결제를 관리하는 시스템이 바로 이러한 역할을 수행한다.

사용자의 불법복제나 Play횟수를 제한하는 사용규칙 제어기능은 대체로 브라우저를 통해서 이루어진다. 그런데 브라우저에는 사용자의 비밀번호 관리프로그램이 들어있기 때문에 이 브라우저으 보안성이 대단히 높아야 한다는 점이 DRM시스템의 성공의 관건이다. 최근에는 실행 파일을 역으로 작동시켜 소스 코드를 복원하는 tempering기술이 많이 발달되어 이를 방지하기 위한 temper-proofing 기술이 필요하다. 사실상 DRM시스템의 안전성은 이 브라우저의 안전성에 달려 있다고 해도 과언이 아니다.

DRM이 사용자에게는 단순히 브라우저만을 가진 시스템으로 보이지만 실제로는 대단히 복잡하고 많은 시스템이 연동되어 돌아가고 있다. DRM이 사용자들의 요청을 받아들여 저작물을 보내려면 키관리 시스템(KMS: Key Management System)과 지불 연계시스템(Payment Gateway), 저작물 관리 DB, 공연규칙 DB, 저작물 사용권 이전을 위한 Super Distribution 서버가 있어야 한다.

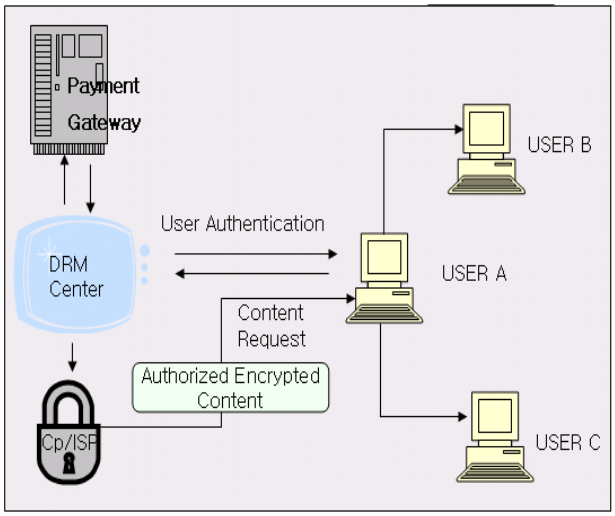
키 관리 시스템(KMS)에서는 등록된 사용자만 접근을 허용하고 불법적인 사용자에게는 시스템에 접근하지 못하도록 사용자 ID와 패스워드를 확인하는 기능을 가지고 있다.[1][2][3][4]

2.3 DRM 과금 결제 기술

지불 연계 시스템 (Payment Gateway)에서는 앞에서 설명된 사용규칙 제어와 밀접한 관련이 있다. 일회성 컨텐츠의 가격과 무한정 재생이 가능한 컨텐츠의 가격, 양도가 가능한 컨텐츠의 가격이 각각 따로 정해져서 과금 되어야 하며 신용카드, 지로, 전자 지갑, 사이버 머니, 은행 자동 이체 등의 다양한 지불 수단을 연결할 수 있어야 하며 저작물을 제공하기 이전에 지불 승인을 먼저 받는 것이

일반적이다.

대부분의 경우 사용자의 비밀번호 혹은 ID를 가지고 컨텐츠를 서버에서 암호화하고 이를 사용자에게 보낸 다음, 사용자측의 컴퓨터에 설치된 브라우저를 통해서 플레이(Play)시 복호화가 진행된다. 얼마 전까지만 하여도 암호화 알고리즘의 보안성에 대한 논란이 있었으나 최근 암호화 알고리즘 중에는 수학적으로 보안성이 증명된 공개 알고리즘이 많이 나와 있기 때문에 DRM 시스템에서의 알고리즘의 보안성에 대한 논란은 많지 않다.[10]



[그림 1] DRM 저작물 유통서비스 흐름도

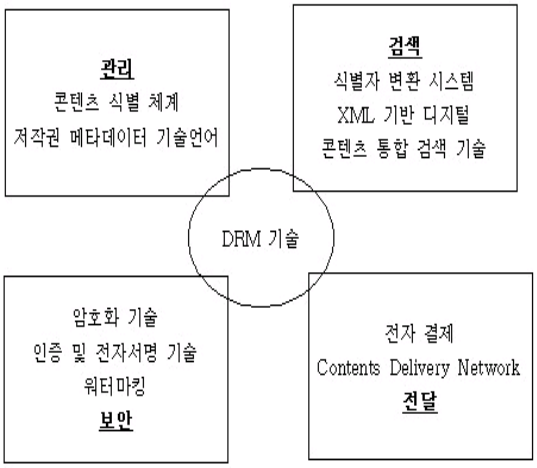
2.4 표준화 대상 기술

- DRM 핵심기술은 디지털콘텐츠의 모든 유통 흐름 속에서 지속적으로 적용되어 디지털콘텐츠의 저작권 보호 및 올바른 거래. 분배. 사용이 이루어져야 할 뿐만 아니라 유통 시장의각 주체들이 다루기 쉽고 일관된 방법으로 기술을 사용 및 적용 가능해야 한다.
- 디지털콘텐츠 산업 시장이 매우 거대하고 디지털콘텐츠의 미디어 형태가 다양한 만큼 디지털콘텐츠 유통 시장의 각 주체들이 서로 다른 DRM 기술을 제안. 적용함으로써 서로 다른DRM 기술이 적용된 디지털콘텐츠의 사용 및 처리에 대한 상호호환성 및 상호운용성이 매우 낮다.
- 서로 다른 DRM 기술에 대한 상호호환성 및 상호운용성을 높이기 위한 표준화 대상 기술을 디지털콘텐츠 식별체계, 디지털콘텐츠 전자상거래 메타데이터, 디지털콘텐츠 유통 모델, 디지털콘텐츠 보호기술로 구분할 수 있다.

3. 연관 기술 분석

디지털콘텐츠 저작권 보호 시스템과 관련한 연관 기술에 대하여 관리/검색/보안/전달 형태로 분류한다.

- 관리: 디지털콘텐츠와 권리정보의 체계적인 분류를 통한 식별 체계의 정의와 저작권 메타데이터 언어 및 데이터 요소를 정의함으로써 정보에 대한 저장, 접근, 검색, 활용이 용이하도록 지원하는 하드웨어/네트워크 및 소프트웨어 기술이다.
- 검색: 디지털콘텐츠 및 권리정보에 대한 접근, 검색을 용이하고 정확하게 하기 위한 식별자/위치정보 변환 기술, 이기종 콘텐츠 통합검색 기술 등을 포함한다.
- 보호: 디지털콘텐츠가 의도한 사용규칙에 따라 이용될 수 있도록 제어하고 불법복제 및 무단이용을 방지하기 위한 디지털콘텐츠 보호 기술과 데이터의 무결성, 기밀성을 보장하며 허가받지 않은 접근을 차단하기 위한 각종 보안 기술 등이 포함된다.
- 전달: 디지털콘텐츠를 이용자에게 원활하게 전달하기 위한 각종 전달 기술과 디지털콘텐츠에 대한 사용료 회수 및 배분을 지원하는 지불관리 기술이 포함된다.[7][8][9]



[그림 2] DRM 연관기술 관계도

4. 적용 분야 및 사례와 국내업계 동향

DRM 기술의 적용분야는 매우 광범위하다. 암복호화 기술을 응용해서 디지털 데이터의 유출을 방지하고 정당한 사용자만이 이를 접근할 수 있도록 개발된 시스템이 DRM이기 때문이다. DRM 기술은 암복호화 기술을 이용해서 디지털로 존재하는 모든 데이터들의 접근을 제어할 수 있는데, 여기에는 오디오, 이미지, 비디오와 같은 멀티미디어 데이터 뿐만 아니라 디지털 문서와 각종 데이터베이스를 포괄할 수 있다.

DRM 기술과 워터마킹 기술을 이용한 지적재산권 보호를 위한 많은 프로젝트가 유럽연합의 지원에 의해서 이루어져왔다. 이들 프로젝트는 DRM 기술과 워터마킹 기술을 활용하기 위한 모델을 개발하는데 주력하였는데 현재까지의 결과로서는

IMPRIMATUR가 실증적 모델로서 인정을 받고 있다. 본 절에서는 IMPRIMATUR의 비즈니스 모델에 대해서 간략하게 소개하기로 하겠다.

IMPRIMATUR의 비즈니스 모델에서는 다음의 기능을 제공하는 것을 목표로 하고 있다.

- 저작물의 상거래
- 저작물의 저작권 보호
- 저작물에 대한 접근제어
- 저작물과 관련된 저작자의 권리를 영역, 매체, 기간에 대해 표현
- 지적재산권 데이터베이스에 의거 추가적 권리 소유자를 고려할 수 있고, 이에 따른 저작권 사용료거래를 지원
- 지적재산권 데이터베이스에 의거 저작물과 관련된 사용권한과 각 저작물에 대해 지불 받는 저작권 사용료의 양을 명시
- 디지털 데이터를 팔 때, 구매자를 구별할 수 있는 복사본을 생성하여 추적
- ECMS (Electronic Copyright Management System)에 참여한 각 개체들과 관련한 지불데이터 흐름의 확인
- 저작물의 사용권한이 적법하다는 사실에 관한 기록을 보관
- 분쟁이 발생 시 저작물의 적법성 증명

이러한 비즈니스 모델에 참여하는 개체별 기능과 특징은 [표 1]과 같다.

참여 개체	기능 및 특징
저작자(Creator)	데이터를 창작
저작물 제공자(Creation Provider)	창작된 저작물의 상업적 이용 제공
미디어 분배자(Media Distributor)	저작물의 분배
소유권자(Rights Holder)	지적재산권의 소유자
구매자(Purchaser)	저작물 구입자
고유번호 발행자(Unique Number Issuer)	저작물에 고유번호 제공
지적재산권 데이터베이스(IPR Database)	지적재산권의 소유권에 대한 현재 정보 유지
인증기관(Certificate Authority)	미디어 분배자와 구매자 인증
은행(Bank)	지불과 관련된 편의 제공
모니터링 서비스 제공자(Monitoring Service Provider)	데이터의 합법적 사용여부 확인

[표 1] IMPRIMATUR 비즈니스 모델 참여개체의 기능 및 특징

DRM기술은 메시지와 컨텐츠의 안전한 전달에 목표를 두고 있기 때문에 여러 분야의 직접적인 응용이 가능하다.

국내에 DRM업계 동향을 보면 토종 3개사인 마크애니, 파수닷컴, 소프트캠프가 시장의 약 95%를 장악하고 있다. 실제로 DRM 프로바이더가 되기란 쉽지 않다. 시장 장벽이 다른 솔루션에 비해 상당히 높고 고객사마다 요구조건을 수용해야 하며 기업 전체시스템을 파악해야 하기 때문에 상당한 시간과 준비가 필요하다. 기술적 수준도 디지털 컨텐츠 생성과정에서 부터 유통과 폐기까지 전과정에 걸쳐있으며 특히 컨텐츠 보안과 밀접한 관련이 있어 약간에 문제점에도 심각하게 회사에 신뢰도에 영향을 미칠 수 있기 때문에 각 회사마다 축적된 기술과 경험이 전제 되어져야 한다.

국내 시장을 살펴보면 대부분 전사차원으로 구축함으로 타 업체 제품으로 교체하기가 쉽지 않다.
그러므로 기존 업체에 대한 충성도가 높다. 이러한 문제점 때문에 다른 업체와 상호 기술적인 호환과 결합이 어려운 단점이 발생한다.

국내 업체들의 DRM 기술수준은 세계 일류급이라는 평가를 받고 있다. 또한 국내 고객들의 요구 수준이 해외보다 월등히 높아 기술의 진화가 빠르다.

현재 국내 보안시장의 최대 이슈는 통합이다. IPS,방화벽, 안티바이러스 등 각기 다르게 성장해 온 기능들이 모여 흔히 UTM이라고 불리는 원스톱 체계를 갖춰가는 추세이다. 최근에는 사전예방은 물론, 사고가 발생해도 추적할 수 있는 길을 열어 놓고 있다. 유통과정 보안은 사용권한 통제와 워터마킹을 통한 출력물 관리가 대표적이다. 워터마킹은 보안문서 출력 시 해당내역 로그를 DB에 전달하는 한편, 출력물에는 지정된 마킹을 삽입한다. 이렇게 특수 마킹을 삽입하면 출력물이 수차례 복사돼도 소유권을 주장할 수 있다. 이는 문서 활용에는 전혀 지장을 주지 않으면서도 원본 출처나 복제경로를 찾아내는데 효과를 발휘한다.

5. 결론

21세기 디지털 컨텐츠가 중요한 하나의 국가적인 아이템으로 자리잡아가 있는 시점에서 이를 보호하고 관리하기 위한 DRM의 발전은 필수적이라고 할 수 있다.

우리나라 DRM 기술이 국제 표준으로 채택되지는 않았지만 세계에서 선도적 기술을 갖고 있다고 볼 수 있다. 그만큼 국내의 기술 수준과 고객 요구 사항이 빠르게 변화하고 있다는 뜻이다.

기술적인 결함과 보완의 취약함은 현시점에서 거의 극복되어 졌다고 판단할 수 있다.

하지만 통합 솔루션으로서 생성부터 폐기까지 전과정에 걸쳐 완전한 관리가 이루어져야 한다.

또한 여러 개의 회사로 나누어져 있는 DRM 업체간에 기술 공유와 함께 기술적 표준이 이루어져 제품 간에 상호호완성도 함께 이루어져야 하며 고객위주의 서비스 편의성도 제공되어져야 한다.

DRM 기술이 사전 예방 위주였다면 사전예방 뿐만 아니라 사고가 발생한 사후에도 추적하고 보호 할 수 있는 기술적 진보에 더욱 매진해야 한다.

참고 문헌

[1] Yong H. Lee, Su H. Dong and Dae J. Hwang,"Design and Implementation of Digital Rights Management System of KERIS," Proc. of SCI2001 Conference Orlando, FL, USA, July 22-25,, 2001.

[2] Kyung S. Yi, Yong H. Lee and Dae J. Hwang,"implementation of Digital Rights Management System using Active Resource Protection Agent, "Proc. of SCI2001 Conference, Orlando, FL, USA, July 22-25, 2001.

[3] Sun M. Jung, Young M. Kim and Dae J. Hwang, "Implementation of Digital Rights and Protection Rule Database in an Agent based DRM Solution, " Proc. of SCI2001 Conference, Orlando, FL, USA, July 22-25, 2001

[4] WP4, The IMPRIMATURE Business Model, Ver. 2.1 IMPRIMATYRE, IMP/I40391B, 1999.
[5] X.Wang, XrML: Extensible rights Markup Language Spec. Ver. 1.3, ContentGuard, 2000.
[6] http://purl.oclc.org/docs/core
[7] NISO, The Dubliln Core Metadata Element Set(ANSI/NISO Z39.85-200x), 2000
[8] Renato Iannella, Open Digital Rights Language(ODRL) Ver. 0.8, White Paper, IPR System Pty. Ltd., 2000
[9] Ross J. Anderson, "Information Hiding - A Survey," Proc. of IEEE, Special Issue on Protection of Multimedia Content, May, 1999
[10] http://www.etri.re.kr
[11] htp://www.drmkorea.org
[12] http://www.markany.com

김 헌
2005년 8월 성균관대학교 컴퓨터공학과 졸업(박사)
2005년 9월 한신대학교 교양전산 초빙교수
관심분야 : 멀티미디어, 디지털 콘텐츠, 문서 및 소스코드 표절 탐지, 인공지능, Bio-Technology