안전한 DRM 키 관리를 위한 비밀 분산 관리 시스템 설계

성 경*

Design of CEK Distributed Management System for Secure DRM Key Management.

Kyung Sung*

요 약

컴퓨터 보급의 증가와 인터넷의 발전으로 다양한 종류와 다량의 디지털 데이터들이 제작, 유포되고 있다. 디지털 컨텐츠는 기존의 아날로그 컨텐츠와 비교할 때 생성, 가공, 유통, 분배 등의 측면에서 많은 장점을 갖는 반면, 원본과 동일한 복사본을 쉽게 생성할 수 있는 특징 때문에 디지털 창작물에 대한 저작권 보호가 중요한 문제로 대두된다. 최근 디지털 컨텐츠 보호의 기술로 DRM(Digital Rights Management)이 사용되고 있으나 컨텐츠 유통 시 키 관리에서 취약성을 띄고 있다. 따라서 본 논문은 디지털 컨텐츠 보호 기술인 DRM을 분석하고 컨텐츠 유통의 키 관리 문제에 대한 개선책으로 *CDMS(CEK Distributed Management System)를 설계하여 이를 이용한 보다 안전한 키 관리 체계를 연구한다.

ABSTRACT

With the spread of computer and development of internet service, the varied contents and digital data has been produced, then provided.
The digital contents are more efficiently able to be created, produced, provided as well as distributed, on the other hand, its own copyrights seem to be more easily broken than analogue contents due to the convenience to make copies of original contents. Therefore, protecting copyrights recently become the key issue.
DRM(Digital Rights Management) is the current technology to protect digital contents from duplication but it sometimes causes problems in the key-management.
In this thesis, we would first like to analyze DRM and find out some trouble in the key-management of it. Finally, we will show CDMS(CEK Distributed Management System) to improve DRM out of the key-management problem and continue to study for better key-management system with it.

키워드
DRM, 비밀분산, CEK, Superdistribution

Ⅰ. 서 론

DRM(Digital Right Management)이란 디지털 저작권에 대한 관리를 뜻한다. E-Book, Game, 음

*한국목원대학교
접수일자 2004. 10. 21

악, 영상, 이미지 등 디지털방식으로 제작된 모든 형태의 저작물을 디지털 컨텐츠라 하고, DRM은 이러한 디지털 컨텐츠의 무단 유통을 방지하는 총체적 기술을 의미한다.

2004년 현재 디지털 컨텐츠의 국내 시장규모만도 3조원에 육박할 것으로 예상되고 있지만, 대규모 시장에도 불구하고 제작자의 저작권 및 컨텐츠 사용자 권한 보호 측면에서는 많은 취약성을 갖고 있는 현실이다. 그 한 예로 DRM을 통한 Forward Lock 방식으로 암호화를 거친 컨텐츠의 경우에도 전송받은 사용자에 의한 재배포가 가능하다는 커다란 문제점을 안고 있다[1].

본 논문은 현재 DRM 솔루션이 갖고 있는 여러 문제점들에 대하여 알아보고, 도출된 문제점을 토대로 보다 안전한 형태의 DRM기술을 위한 CEK(Content Encryption Key)관리에 있어 분산관리방식의 시스템 설계와 CEK 분배 프로토콜 제안을 목적으로 한다. 이를 위하여 2장에서는 관련연구로 DRM 기술과 키 관리에서 발생하는 문제점을 알아보고, 3장에서는 CEK 분산관리시스템 설계를 위한 배경기술이 되는 비밀분산 방법에 대해 알아본 후, CEK 분산관리 시스템 설계하고. CEK 분배 프로토콜을 제안한다. 마지막으로 4장에선 결론 및 향후 연구방안으로 끝을 맺는다[2][3].

II. 관련연구

DRM 기술이란 암호화된 컨텐츠를 배포함으로써 비인가자의 사용을 금하도록 보호하는 총체적 기술로, 크게 저작권 보호기술과 컨텐츠 관리 기술로 나눌 수 있다[4]. 이번 장에서는 저작권 관리기술 및 컨텐츠 보호기술에 대하여 설명하고 일련의 기술을 이용한 DRM 이용 시 발생할 수 있는 Key 관리 문제에 대해서 알아본다.

2.1 저작권 보호기술

저작권 관리기술에서 정의하는 일련의 원칙과 시나리오들을 강제화(Enforcement) 하는 기술로서 암호 기술, TRM(Tamper Resistant Module) 및 키 분배 및 관리 기술 등이 있다.

① 컨텐츠 암호화 기술

디지털컨텐츠의 보호를 위한 암·복호화 응용 기술, 거래 당사자 간의 지적재산권에 대한 인증 및 전자서명 기술, 내용 제어를 위한 워터마킹 및 핑거 프린팅 기술을 의미한다. 중요 표준화 대상항목으로는 암호화 된 컨텐츠 포맷의 표준, 컨텐츠 암호화 기술 및 규격, 워터마킹 응용의 분류, 평가 기준 및 절차의 표준화 등을 들 수 있다.

② 인증 기술

신원확인, 프로세스, 시스템의 무결성 등을 보장하는 인증 기술과 송신자와 수신자의 데이터 발신 및 수신을 증명할 수 있는 부인 방지, 그리고 서명키 생성 등에 관한 기술을 의미한다.

클리어링 하우스(라이센스 서버)를 이용하여 사용자의 인증에 관한 정보를 처리하는 것이 일반적이며, 최근에는 수준 높은 인증 처리 기술을 바탕으로 인증 절차를 단순화하는 것에 초점을 맞추고 있다.

인증은 임의의 정보에 접근할 수 있는 주체의 능력이나 자격을 검증하는데 사용되는 수단이자 시스템의 부당한 사용이나 정보의 부당한 전송 등을 제어하기 위한 목적으로 사용되며, 다음의 세 가지 방식으로 사용될 수 있다.

첫째, 아는 것에 대한 인증(Authentication by knowledge)

- 패스워드 인증방식, 암호 구 인증방식, 일회용 패스워드, 도전-응답 프로토콜

둘째, 소유하고 있는 것에 대한 인증(Authentication by ownership)

- 자기 테이프 카드 혹은 Smart card 이용

셋째, 개체의 특성에 의한 인증(Authentication by characteristic)

- 지문, 장문, 홍채 등의 신체적 특성을 이용하며, 음성, 서명, 동작 등의 행위적 특성을 이용

③ 키 분배 및 관리

DRM 키 분배 방법은 대칭키 방식과 공개키 방식으로 구별될 수 있다. 대칭키 방식은 하나의 키 분배 서버로 모든 부하가 집중되고 모든 컨텐츠 거래에서 키 분배 서버가 관여하게 되며, 반면 공개키 방식을 사용할 경우 분산성, 확장성, 상호 운용성 등에서 많은 장점을 갖게 되나, 공개키 기반구조(PKI)가 필요하다는 부담이 있다. 현제 제안되고 있는 방식은 두 암호 시스템이 갖는 장점만을 이용하여 실제 데이터의 암호에는 대칭키 방식을, 대칭키 방식에 이용되는 비밀키의 암호에는 공개키 방식을 이용하는 하이브리드 암호 시스템(Hybrid cryptosystem)이 주로 이용된다.

2.2 컨텐츠 관리기술

컨텐츠 관리기술로는 DOI(Digital Object Identifier)와 컨텐츠 메타 데이터, ODRL (Open Digital Rights Language)등이 있으며 이들은 컨텐츠의 고유 정보와, 사용자의 권리명세 등을 나타낼 때 사용하는 방식이다.

① 디지털컨텐츠 식별 시스템

디지털컨텐츠의 체계적인 관리 및 통제, 접근, 이용효율성을 위해 대상물을 식별할 수 있는 체계 및 변환시스템을 말한다. 대표적인 디지털컨텐츠 식별 시스템인 DOI(Digital Object Identifier)는 현재 웹 자원에 대한 Unique identifier 와 URL 을 보완한 URN(Unform Resource Name) 체계를 만족시키는 방향으로 전개되고 있다. DOI의 구조상 글로벌 핸들링을 맡는 미국의 CNRI(Corporation for National Research Initiatives)와 각 지역별로 URL로의 변환 서비스를 담당하는 RA(Registration Agency)가 필요하다. 이처럼 디지털컨텐츠에 고유한 코드를 부여하는 기술인 관계로 아직 표준화 단계까지는 시간이 소요될 것으로 예상되며, 이에 따라 대다수의 DRM 솔루션들은 DOI 체계를 미적용 상태에 있다. 따라서 디지털컨텐츠 식별체계와 식별체계간의 상호연동 기술 및 변환 시스템의 개발이 절실히 요구되고 있다.

② 컨텐츠 메타데이터

디지털컨텐츠 메타데이터는 디지털컨텐츠에 대한 식별정보, 내용정보, 특성정보, 저작권 정보 등의 요소를 정의하고 기술하기 위한 언어이다. 컨텐츠 메타데이터는 점점 확장되어 복잡성을 띠게 될 컨텐츠 비즈니스를 원활하게 지원하기 위해 유럽연합의 지적재산권 관련기관에서 시작된INDECS (Interoperability of Data in E-Commerce System)를 중심으로 논의가 진행 중에 있다. XrML 이나 DOI 역시 메타데이터의 구조를 띄고 있으며, 궁극적으로는 전자상거래에서 투명한 상거래와 저작권료를 받을 수 있는 컨텐츠 유통 프레임워크와의 호환 구조를 창출하는 것이 목적이다. 중요 표준화 대상항목으로는 메타 데이터간 상호 운용성을 위한 프레임워크 개발, 전자상거래 메타데이터 기술언어 개발, RDD와 REL 개발 및 표준화 등이 있다. 메타데이터 기술언어는 다음과 같다.

. XrML(eXtensible rights Markup Language)

3C SGML WG에서 제안되고 Content Guard에 의해 개발된 XrML은 현재 가장 많이 사용되는 XML 기반의 저작권 표현 언어이다. XrML은 디지털 컨텐츠 및 웹 서비스와 관련된 권리와 조건들을 표현하고, 저작권자, 컨텐츠 제공자, 사용자간에 권리항목들의 표준을 제정하기 위한 목적에서 시작되었다.

컨텐츠 제공자는 XrML을 이용하여 사용자에게 특정 권한을 부여할 수 있으며, 이러한 모든 권한에 대해서 사용기간과 조건을 명시할 수 있다. 또한 사용기간과 사용권한에 따른 과금이 가능하다.

③ ODRL(Open Digital Rights Language)

ODRL은 컨텐츠에 대한 권리정보를 표현하기 위하여 정의된 표준 언어 및 어휘이다. 권리언어를 표현하는 ODRL Expression Language와 데이터 사전에 들어가는 요소들을 정의하는 ODRL Data Dictionary가 표준화의 대상이며, 모두 XML schema 를 사용하여 표현된다.

ODRL 은 다음의 구성요소를 사용한다.

- Assets: 유일하게 식별될 수 있는 컨텐츠(식별자, 암호화 정보 등)
- Rights

. Permission: Asset에 대해 허용되는 서비스(play, print, view 등) 명세

. Constraints: Permission에 대한 제약사항(사용회수, 기간, 지역 등) 명세

. Requirements: Permission을 얻기 위한 전제조건(Per-, Pre-Pay 등) 명세

. Conditions: Permission을 위해 만족하지 말아야 하는 조건 명세

- Parties: Asset과 Rights에 대해 어떤 형식의 소유권을 주장할 수 있는 사용자, 역할, 그리고 권리 보유자를 명세

2.3 키 교환 및 관리의 문제점

DRM 시스템에서 저작권 보호의 핵심 요소기술인 암호화를 이용한 컨텐츠 유통 시 다음과 같은 사항들에 대하여 고려해야 한다.

첫째, 컨텐츠의 암·복호화에 쓰이는 Key는 어디에 저장할 것인가? 이것은 Key의 저장위치에 따라 컨텐츠 보호가 불가능 할 수도 있는 이유가 되기 때문이다. 이미 다운로드된 컨텐츠와 이를 복호화 시킬 수 있는 Key를 갖고 있는 사용자라면 얼마든지 무단 배포가 가능하기 때문이다.

둘째, 사용권과 소유권 분리의 문제. 만약 컨텐츠에 대하여 소유권을 갖고 있지 않고 단지 재생에 대한 사용권만을 인정받은 사용자라면 재생횟수에 대한 제한을 위해선 특수한 Key 관리방식의 시스템을 필요로 한다.

셋째, 어떤 방식으로 재생에 대한 보호를 할 것인가? 사용자가 다운로드 받은 컨텐츠를 재생할 때 CP가 처음에 제공 했던 원본 컨텐츠의 질(Quality)의 변화 없이 사용자의 Player에서 재생이 가능한지에 대한 문제이다. 이것은 처리 성능이 좋은 일반적인 PC 보다는 PDA나 혹은 모바일 환경에 적용되는 문제로써, 암·복호 시 시스템에서 발생 하게 되는 부화에 대한 처리가 가능한가의 문제라 할 수 있다.

이상의 고려사항외에도 과금 및 결제의 문제, 컨텐츠의 불법적인 수정과 도용의 문제, 등 여러 가지 문제점들을 나열 할 수 있다[5]. 이러한 고려사

항과 더불어 여러 문제점들 대부분이 Key 교환 및 관리를 통해 보안될 수 있는 문제이기에 다음 장에선 Key 관리에 대한 보다 안정적인 방식에 대하여 제안하게 된다.

그림 1. DRM Key 관리의 문제점
Fig 1. DRM Key Management Problem

III. CEK 분산 관리 시스템 설계 및 분배 프로토콜 제안

앞장에서 설명된 바와 같이 DRM은 컨텐츠 제작 후 유통 및 이용 시 Key 관리에 따른 여러 가지 문제점을 안고 있다. 이번 장에서는 이러한 문제점에 대한 해결책으로 CEK 분산 관리 시스템을 설계하고 이를 이용한 CEK 분배 프로토콜을 제안한다.

3.1 비밀분산법

기밀을 요하는 정보를 안전하게 유지, 관리 하기 위한 암호 프로토콜의 일종으로 하나의 비밀정보를 다수의 조각으로 분할하여 다수에게 공유시킴으로써 원 정보를 보다 안전하게 유지, 관리하는 방식이다[6].

비밀정보 K에 대하여 분할된 다수의 조각을 비밀조각이라 하고, 비밀조각을 생성하고 분배하는 사람을 분배자(Dealer), 생성된 비밀조각을 공유하는 사람을 참가자라 한다.

- n : 참가자의 수
- P : 비밀 분배에 참가하는 참가자 Pi (1≤i≤n)
- q : 소수
- k : 비밀정보 ∈ Zq
- K : 비밀정보 k의 집합
- spi : 비밀조각 ∈ Zq
- Spi : 각 참가자 Pi가 갖고 있는 비밀조각 spi 의 집합

① 비밀값 분산

1. 분배자는 적당한 임의의 소수 q (q≥ n+1)를 선택한다.

2. 서로 다른 a1, a2, ..., at-1 (ai ∈ Zq, 1≤i≤ t-1)를 임의적으로 선택

3. 분배자는 자신의 비밀정보 k=a0를 상수항으로 하는 임의의 (t-1)차 다항식

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$$

(mod q)를 선택

4. 분배자는 비밀조각 $s_{pi} = f(x_i)$를 계산하여 각 참가자 Pj 에게 (x_j, s_p) $(1 \le j \le n)$를 보낸다.

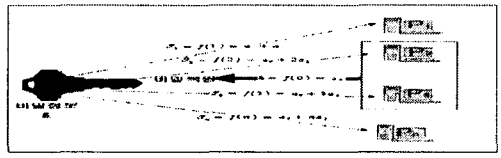

그림 2. (2,n)-비밀분산 방식의 예
Fig 2. (2n)-CEK distributed mode example

② 비밀정보 복원

비밀정보를 복원하기 위해서 모인 임의의 t명의 참가자들을 $P_{A1}, \ldots, P_{At}$라고 하고, 이들의 비밀조각을 $S_{P_{A1}}, \ldots, S_{P_{At}}$라고 한다. 참가자들은 그들의 비밀조각 $S_{P_{A1}} = f(x_{A1}), \ldots, S_{P_{At}} = f(x_{At})$를 입력 값으로 $f(0) = k$를 복원한다.

$f(0) = \sum_{i=1}^{t} s_{p_{Ai}} \Pi \prod_{j=1, j \neq i}^{t} \frac{x_{Aj}}{(x_{Aj} - x_{Ai})} \ (mod\ q)$ 를 구한다.

[그림 2]는 비밀분산 방식의 예로 분배자에 의한 임의로 선택한 1차 다항식 $f(0) = a_0 + a_1 x$에 의해 생성된 비밀조각 $s_n = f(x_j)$ $(1 \le j \le n)$으로부터 임의의 명의참가자들이 모여 비밀 정보$k = a_0$를 복원한다.

단 $x_j = j (1 \le j \le n)$

3.2 CEK 분배 관리 시스템 개요

일반적인 DRM 동작을 살펴보면 컨텐츠를 가진 공급자(CP)와 지불 시스템을 연결하여 컨텐츠를 제공하며 사용자에게는 암호화하여 저작물을 전달한다. 사용자의 다운로드 요청 후 DRM 서버에서 인증기관을 통한 인증절차를 거친 인증서가 사용자에게 발급되고 원하는 컨텐츠를 신청 후 지불을 마치게 되면 지불시스템에서는 지불 승인을 DRM 서버에게 통보한다. 그 다음으론 CEK를 사용하여 암호화한 컨텐츠를 사용자에게 전송함으로써 오직 허가된 사용자만이 사용가능한 컨텐츠가 제공되는 절차로 이루어 졌다. 본 논문은 이러한 일반적인 DRM 과정에서 CEK를 관리하는 Sever를 별도로 구성하여 CEK 관리상 생길 수 있는 취약점을 보완한다.

CEK를 이용한 암호화 기법을 이용한 컨텐츠 관리는 크게 암호화 작업과 복호화 작업의 두 단계로

나눌 수 있다. 암호화 작업은 컨텐츠에 대한 Packaging시 컨텐츠 서버와 라이선스 서버에서 함께 수행 되고 복호화의 경우 컨텐츠 이용 시 사용자의 기기 내에서 수행되는 작업이다. 여기서 만약 디지털 컨텐츠의 유통 전반에 참여하는 CP, 라이선스서버, 소비자 등의 모든 구성요소들이 비밀키를 알 수 없도록 관리하는 방법이 가능하다면 CEK에 대한 불법적인 접근을 막을 수 있음을 착안하여 이를 이용한 CEK 분배 관리 방식을 제안 한다. 이는 자신의 키에 접근할 수 없다면 알고리즘의 비밀성이 보장되는 한 컨텐츠의 불법적 사용(불법 복제를 이용한 무단유포)이 불가능하기 때문에 가장 원천적으로 비밀키 노출에 대한 취약성을 해결할 수 있는 방법이 된다.

컨텐츠 제공자(CP)와 n개의 비밀키 관리 시스템이 있다고 가정했을 때, CP가 갖고 있는 모든 m으로 비밀키를 복구 할 수 있도록, 그러나 CP 외에 어떠한 m-1부분도 그 비밀키에 대한 정보를 나타낼 수 없도록 비밀키를 n 부분으로 나누고 각 관리 시스템들에 분산시킨다. m과 n값을 각기 다른 값을 선택하면 보안및 신뢰도가 서로의 지위를 교환하는데 영향을 미치게 된다. CEK 분산 관리 시스템은 어떠한 그룹도 단독적으로 완전한 비밀키에 대하여 예측하지 못하게 함이 기술의 중심사항이다.

3.3 CEK 분배 관리 시스템 설계

SDMS의 구성은 각각의 분산된 키들을 관리하는 키 분산 서버와 키 분산서버들의 정보 및 총괄적 관리를 수행하는 관리 서버(Management Server)로 구성된다.

제안되는 CEK 분배 관리 방식은 CP의 클리어링하우스 에서 CEK를 생성하고 이를 이용 컨텐츠를 Packaging하는 과정까지는 기존의 DRM 방식과 동일하다. 하지만 CDMS(CEK Distributed Management System)에서 CEK의 정보를 n개로 나누고 이를 분배해서 관리한다는 점에서 분명한 차이를 둘 수 있다.

생성된 CEK를 K라 하면 이를 n개로 나누어 $(S_{p1}, S_{p2}...S_{pn}) \in K$ 각각의 분배 서버들이 나눠 갖게 되고 관리서버에서는 분배된 키 값에 대한 Index정보만을 갖고 있게 된다. 이렇게 CEK가 생성 분배된 다음 암호화된 컨텐츠가 사용자에게 제공되고, CEK에 대한 Index 정보가 포함된 데이터를 인증서를 통하여 암호화하여 사용자에게 발송하게 되는데 여기까지를 CDMS 부분이 수행하게 된다.

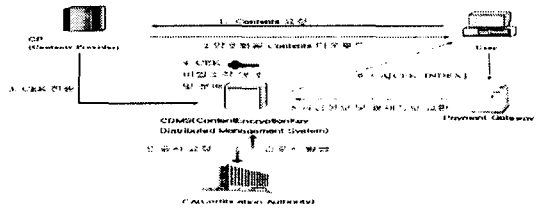

그림 3. CEK 분배관리 시스템 구성도
Fig 3. CEK Distributed management system configuration

사용자는 전송 받은 컨텐츠를 복호화 시켜 이용하게 되는데 이 부분은 DRM 에이전트에서 수행하게 된다. DRM 에이전트는 다운 받은 컨텐츠 라이선스에서 추출한 CEK Index 정보를 가지고 분배된 CEK를 조합하게 되는데 그 과정은 다음과 같다.

전송된 Index 값은 각각의 분배 서버들 $(P_1, P_2...P_n)$이 갖고 있는 $(S_{p1}, S_{p2}...S_{pn})$들을 요청하게 되면, 각각의 분배 서버들에서는 사용자 인증에 필요한 정보를 나누어서 검토하게 된다.

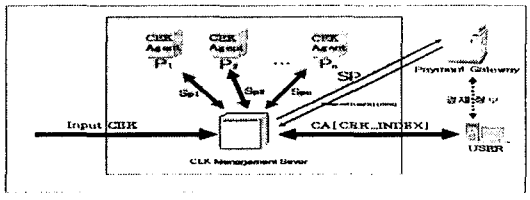

그림 4. CDMS Architecture
Fig 4. CDMS Architecture

이 경우 사용자가 자신이 갖고 있는 Index 정보를 누출하여도 컨텐츠를 사용 시 인증 및 지불이 이뤄지지 않은 상태라면 비밀키를 조합할 수 없게 되므로 키 관리에서 야기되는 문제점에 대한 효율적 대응책으로 적용될 수 있다.

3.4 CEK 분배 프로토콜

CDMS는 컨텐츠 보호와 과금체계 관리 및 Superdistribution의 안전성을 고려하여 CDMS의 프로토콜 체계를 구성하였다. CEK 분배 프로토콜은 크게 분배 프로토콜과 조합 프로토콜로 나눌 수 있다.

사용자는 인증기관에 등록을 요청하고 등록기관에서는 신원 및 기타정보의 조회 후 인증서를 생성하여 사용자의 개인 Key가 첨부된 인증서를 발행한다. 다음으로 사용자는 원하는 컨텐츠를 요청하

게 되면 CP에선 CEK를 이용하여 패키징된 컨텐츠를 제공하고, CDMS에 CEK 정보를 발송한다. CDMS에서는 전달받은 CEK 정보를 비밀조각으로 분배하여 각각의 에이전트들에게 분배하고, 결제정보를 처리하는 Payment Gateway에 마스터 Key 정보인 SP를 전송한다.

여기서 SP는 Payment Gateway에 결제정보가 처리되는 사용자라면 누구나 CEK_INDEX 정보를 송신케 하여 컨텐츠를 이용케 하는 역할을 한다. 이 기능은 Superdistribution을 가능케 한다.

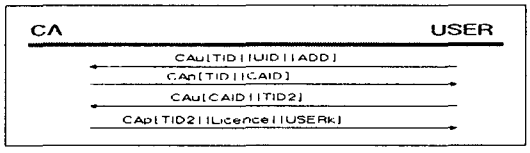

그림 5. Licence 획득 프로토콜
Fig 5. Licence acquisition Protocol

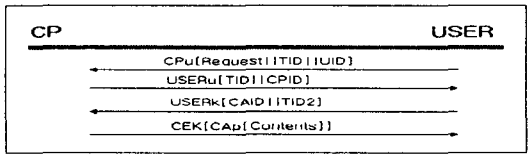

그림 6. Contents Download
Fig 6. Contents Download

다음으로 CEK 분배 프로토콜을 살펴보면 CP로부터 전송된 CEK는 CMS(CEK Management Sever)에서 연산을 거쳐 각각의 에이전트들에게 CEK 비밀조각을 전송함과 동시에 전송된 CEK 비밀조각들의 에이전트 INDEX 정보를 생성 후 Payment Gateway로부터 결제 정보가 들어옴과 동시에 사용자에게 전송된다. 이때 인증기관으로부터 부여받은 사용자 개인키를 이용하여 CEK_INDEX값을 암호화 시키고 인증정보를 첨부한다.

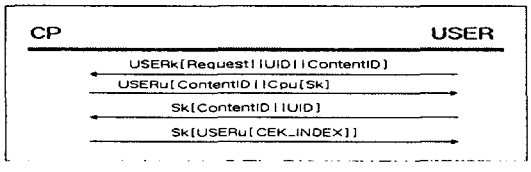

그림 7. CEK_INDEX Download
Fig 7. CEK_INDEX Download

CEK 조합 프로토콜은 사용자가 결제정보를 완료 후 전송받은 CEK_INDEX값을 전송할 경우 CDMS의 CMS는 전송받은 INDEX 값을 갖고 CEK를 복원하여 전송한다. 이때 인증 값을 이용하여 해쉬 과정을 거치게 되는데, 이것은 전송받는 CEK 정보 유출을 방지하기 위함이다. 이제 CEK 해쉬정보를 전송받은 플레이어는 암호학적 점검 값과 비교하여 일치함이 확인될 경우 컨텐츠를 복원 재생을 가능케 한다.

IV. 결 론

디지털 컨텐츠의 제작과 사용이 큰 비중을 차지하는 요즘 보다 신속하고 효율적인 양질의 컨텐츠를 배포시키는 기술이 중점적으로 다뤄지며, 또한 컨텐츠의 안전한 보호 기술 역시 병행해서 발전 돼야할 중요한 과제라 하겠다. 이러한 요구와 부합하여 DRM의 요소 기술들은 현재 활발한 표준화 동향이 연구 되고 있는 추세다.

본 논문은 이러한 추세에 맞춰 비밀분산 암호방식을 기반으로 DRM에서 키 관리 시 발생하는 취약성에 대한 대비책을 제시하기 위하여 CDMS가 제안되었다. 이는 Superdistribution이 요구되는 DRM 시스템에 광범위하게 적용될 수 있으리라 예상된다.

향후 연구방향으로 CDMS에서 CEK_INDEX생성, 전송 및 조합부분에 있어서 생기는 트레픽을 휴대용 단말기 등의 소형 장치에서도 사용이 가능한 경량의 시스템으로의 개발을 들 수 있겠다.

참고문헌

[1] Joshua, D. Susan, K, "Understanding DRM System"An IDC White Paper", IDC, 2001.
[2] 권순홍, "실시간 멀티미디어 서비스의 DRM 적용방법설계",정보과학회 춘계학술대회, VOL.2 NO.01, pp.0481~0483, 2002.04.
[3] 한국 디지털 콘텐츠 포럼, 디지털 유통 프레임워크 구축 및 기술표준 전략 수립에 관한 연구, 2002. 2.
[4] 이창열 "디지털 정보에 대한 식별자 부여 및 전자상거래용 메타데이타 모델에 관한 연구" 한국교육 학술정보원, RR-1999-2
[5] "DRM Forum"

http://www.drm.or.kr/~contents/index.html
[6] E. F. Brickell and D. M. Davenport, "On the Classification of Ideal Secret Sharing Schemes "Journal of Cryptology, Vol. 4, pp. 123-134, 1991.

저자소개

성 경(Kyung Sung)

1988 목원대학교 전자계산학과 (공학사)
1993 경희대학교 전자계산학과 (공학석사)
2003 한남대학교 컴퓨터공학과 (공학박사)
1994~2004 동해대학교 컴퓨터공학과 교수
2004~현재 목원대학교 컴퓨터교육과
※관심분야 : 정보보호 및 정보관리, 컴퓨터네트워크, 신경회로망, 컴퓨터교육