웹서비스 환경에서의 프라이버시를 보호하는 디지털 저작권 관리 아키텍쳐

Web Services-Adaptable Privacy-Aware Digital Rights Management Architecture

송유진(Song You Jin)*, 이동혁(Lee Dong Hyeok)*

초 록

Context-Aware 환경의 유비쿼터스 시대로 들어서게 되면 기존의 DRM 시스템은 디지털 저작권 관리 서비스 제공상의 어려움 즉, 상황에 따른 서비스 제공, 저작권 사용자의 프라이버시 보호 문제가 대두될 수 있다. HKUST에서 제안한 웹서비스 DRM 시스템은 유비쿼터스 환경하의 상황(Context)변화에 적응하도록 디지털 콘텐츠를 적절하게 가공하여 제공할 수 없으며, 사용자에 대한 프라이버시 보호가 불가능하다. 한편, 네덜란드의 필립스 연구소에서도 DRM 시스템의 프라이버시 문제를 지적하고 이에 대한 대안을 제안하였으나 이 논문의 한계점은 사용자와 기기간 전달되는 인증 정보가 노출될 경우 Sniffing/Replay 공격이 가능하여 저작권이 획득 가능하다는 단점이 있다. 본 논문에서는 이러한 단점을 보완하여 유비쿼터스 웹서비스 환경에서 프라이버시를 보호할 수 있는 DRM 아키텍쳐를 설계하였다. 제안한 아키텍쳐는 상황에 따른 서비스 제공이 가능하고 Context-Aware 환경에서 사용자의 익명성을 유지하며 프라이버시를 보호할 수 있다. 또한, Sniffing/Replay 공격에 안전한 사용자 인증 메커니즘 제공이 가능하다. 본 논문의 결과를 활용하여 상황에 따른 디지털 저작권 관리 및 사용자 프라이버시 문제를 해결할 수 있는 웹서비스 DRM 시스템 개발이 가능할 것이다.

ABSTRACT

Current DRM system has limitation in protection of user's privacy. Therefore, many troubles are expected in service providing if it comes into the ubiquitous times of context-aware environment. HKUST proposed a watermark-based web service DRM system. However, the relevant study does not consider ubiquitous environment and cannot provide service that considered a context. And privacy protection of a user is impossible. On the other hand, Netherlands Phillips laboratory indicated a privacy problem of a DRM system and they proposed an alternative method about this. However, in relevant study, a Sniffing/Replay attack is possible if communicated authentication information are exposed between a user and device. We designed web services adaptable privacy-aware DRM architecture which supplements these disadvantages. Our architecture can secure user authentication mechanism for sniffing/Replay attack and keep anonymity and protect privacy. Therefore, we can implement the privacy-aware considered web service DRM system in Context-Aware environment.

키워드 : 웹서비스, DRM, PADRM(Privacy-Aware DRM), OTP, Dynamic Access, XrML

Web Services, DRM, PADRM, Dynamic Access, OTP, XrML

* 동국대학교 대학원 전자상거래학과

1. 서 론

최근 인터넷이 발전되고 대량의 디지털 정보가 유통될 수 있는 환경이 구축됨에 따라 저작권을 가진 콘텐츠가 인터넷 환경에서 사용 가능하도록 디지털 콘텐츠 형태로 제작되고 있다. 디지털 콘텐츠의 제작 과정에서는 원본 아날로그 콘텐츠를 전자적 형태로 제작하고 변환한다. 디지털화 된 자료는 보관과 전달이 용이하며, 정보에 대한 접근이 손쉽게 될 수 있다. 정보의 보급이 손쉽게 되는 것은 디지털화의 커다란 장점이며 저작권을 가진 콘텐츠를 용이하게 유통시킬 수 있다. 따라서 디지털 콘텐츠는 앞으로의 전자상거래 환경에서 주요한 테마로 자리매김 하게 될 것이다.

그러나 디지털 콘텐츠에는 정보 융합 및 복제의 용이성, 광범위하고 신속한 전달성, 통제의 곤란성이 존재한다는 단점이 있다. 이러한 문제를 해결할수 있는 기술로서 핑거프린팅, DTCP(Digital Transmission Content Protection), 워터마킹, DRM(Digital Right Management) 기술 등이 제안되었다. 이 가운데 DRM기술은 디지털 콘텐츠에 대한 불법 사용을 원천적으로 방지할 수 있다. 암호화 기술을 이용해 디지털 콘텐츠를 패키지 형태의 암호화된 데이터로 변환시키는 DRM기술은 디지털 콘텐츠가 전달된 후 사용자 측면에서 제한을 받게 된다. 결과적으로 인증 절차를 거치지 않은 사용자가 우연히 취득했다 하더라도 사용할 수 없다.[4]

HKUST(Hong Kong University Science Tehnology)[2]의 Sai Ho Kwok은 워터마크 기술을 기반으로 한 웹서비스 DRM 시스템을 제안하였다. 워터마크 기술이란 저작권 정보를 디지털 콘텐츠 속에 삽입시켜 소유자의 저작권을 보호하는 것을 목적으로 하는 기술로서, 콘텐츠에 대한 소유권 등을 판별할 수 있는 기술에 해당된다.[3] 이러한 워터마크 기술의 삽입과 추출방법을 차세대 환경인 웹서비스 환경에 적용하였다는 점에서 의의가 크다.

그러나 Sai Ho Kwok이 제안한 방법은 사용자의 프라이버시 문제를 고려하지 않고 있다. DRM 기술은 암호 기술, 키 관리 기술 등이 복합적으로 작용하므로 필수적으로 사용자의 정보가 요구되게 된다. 이러한 정보를 공개하는 것은 개인정보 노출의 문제로 이어질 수 있다. 콘텐츠 사용의 편리를 위해서 사용자의 프라이버시가 침해받게 되는 것은 바람직하지 않다. 아울러 해당 연구는 유비쿼터스 환경을 고려하지 않아 상황(Context)변화에 적응적(Adaptive)으로 디지털 콘텐츠를 적절히 가공할 수 없다. 따라서 사용자의 Context를 고려한 서비스 제공은 불가능하다.

한편, 네덜란드의 필립스 연구소에서는 신원 기반의 DRM 시스템에 대한 문제점을 지적하고 이에 대한 프라이버시 대책을 제안하였다.[1] 해당 연구에서는 디지털 오디오 및 비디오에 대한 내용의 배포에 있어서 발생되는 프라이버시 문제에 중점을 두고 사용자가 언제 어디에서든지 콘텐츠에 접근하는 것을 가능하게 하고 어떠한 장치에도 콘텐츠 제공자에 의해 발행된 증명서를 통하여 익명성을 유지한 상태에서 접근할 수 있게 하였다.

그러나 필립스 연구소가 제안한 프라이버시 보호 시스템은 콘텐츠의 이용자와 콘텐츠

재생 장치, 콘텐츠 제공자의 3가지의 영역에서만 프라이버시 보호 문제를 표현하고 있어 웹서비스와 같은 환경에 실제로 적용하는데 제약이 있다. 또한 사용자와 기기간 전달되는 인증 정보가 노출될 경우 Sniffing/Replay 공격이 가능하다.

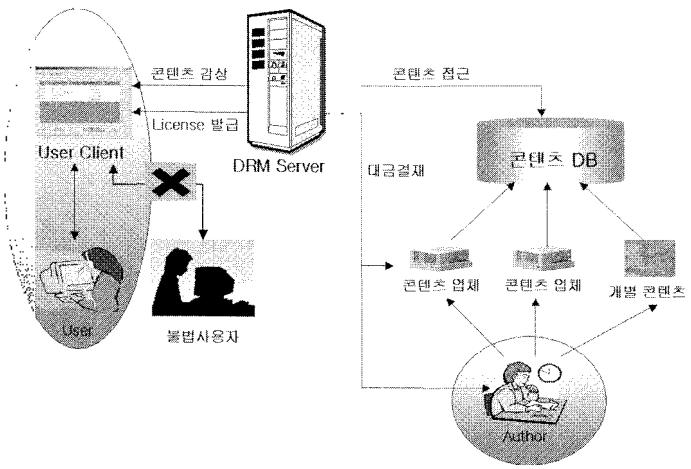
본 논문에서는 이러한 단점을 보완하여 Context-Aware 환경에서 프라이버시 문제를 고려한 웹서비스 DRM 시스템을 제안한다. 제안한 방법은 디지털 콘텐츠의 유통 과정에서 익명성을 제공하여 개인정보를 노출시키지 않으며 안전하게 디지털 콘텐츠에 대한 라이센스 취득이 가능하다. 또한 Sniffing/Replay 공격에 안전한 사용자 인증 메커니즘을 제공하고 Context 정보의 원활한 전달을 통한 상황(Context)에 적응적(Adaptive)으로 콘텐츠를 가공하여 서비스를 제공할 수 있다. 이러한 방법으로 Context-Aware 환경에서 프라이버시 문제를 고려할 수 있는 Dynamic DRM 시스템을 구현할 수 있다.

2. 관련 연구

2.1. 기존의 DRM 시스템

기존의 DRM 시스템은 〈그림 1〉과 같다. DRM 시스템은 콘텐츠 제공자와 사용자의 매개체 역할을 한다. 사용자는 DRM 클라이언트를 이용하여 디지털 콘텐츠를 사용할 수 있다. 콘텐츠 이용은 대금 결제에 따른 라이센스 발급이 전제되며 그렇지 않은 경우 콘텐츠를 이용할 수 없다. 따라서 DRM 서버는 대금을 정상적으로 결제하지 않는 불법 사용자로부터의 콘텐츠에 대한 접근을 차단해 준다. 지급된 대금은 등록한 콘텐츠 업체 및 저작권자에게 배송된다.

Helsinki 연구소에서는 법률적 저작권과 기술적인 요소에 대하여 저작권을 취득하고 중재할 수 있는 DRM 시스템에 대하여 연구하였다.[14] DRM은 디지털 콘텐츠를 가져올



〈그림 1〉 DRM 시스템 구성도

수 있는 방법 중 하나이다. 해당 논문에서는 법률적인 저작권과 요구사항에 기반하여 콘텐츠를 보호할 수 있는 프레임워크를 소개하고 있다.

해당 논문에서는 조직과 생산품의 두가지 단계로 저작권 관리에 대하여 논의하고 있다. 두가지의 단계는 밀접하게 연관되어 있으며 상호 의존하고 있다. 저작권 관리는 최소 다음과 같은 기능이 요구된다.

- 저작권 관리 정책을 지정하고 수정 가능하여야 한다.
- 상호 동의를 취하고 그 과정을 중재할 수 있어야 한다.
- 취득한 저작권의 정보를 관리할 수 있어야 한다.
- 라이센스 정보를 제어하고 발급할 수 있어야 한다.
- 여러 상이한 비즈니스 모델 아래 매매가 가능하여야 한다.
- 수익을 분배할 수 있어야 한다.
- 콘텐츠의 분실 등 위험에 대처할 수 있어야 한다.

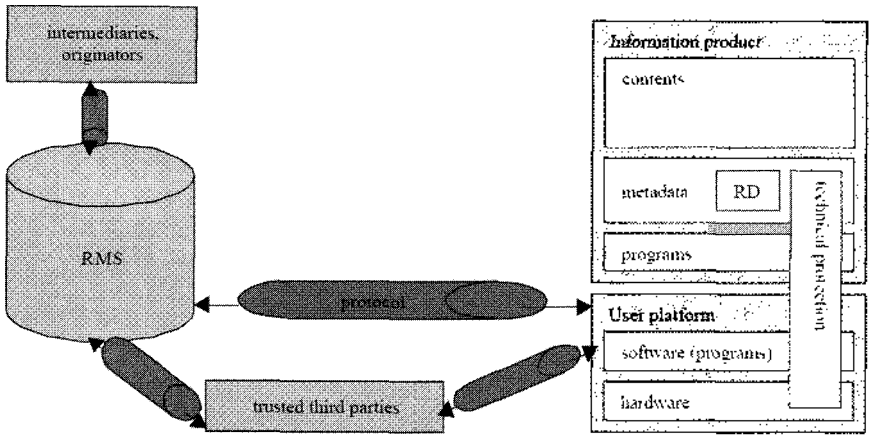
조직 레벨에서의 저작권 관리 시스템은 위와 같은 요구사항을 만족할 수 있어야 한다. 〈그림 2〉에서는 사용자 플랫폼과 정보 제공자의 상호작용을 나타내고 있다.

RMS(Right Management System)는 정보 제공자와 사용자간 매개 역할을 한다. Information Products는 콘텐츠나 메타 데이터 및 프로그램을 의미한다. 사용자는 Information Product에 사용자 플랫폼을 통하여 접근한다. 기술적 보호 도구는 상호간 정보 전달 과정에서 통신 프로토콜로 사용될 수 있다.

그러나 기존의 연구에서는 다음과 같은 한계점이 존재한다.

① Context-Aware 환경을 고려하지 않음

유비쿼터스 시대로 나아감에 따라, 사용자



〈그림 2〉 Helsinki 연구소의 DRM Framework[14]

의 Context에 대한 고려가 필히 요구된다. 사용자의 현재 상황, 시간, 장치 등에 따라 디지털 콘텐츠의 내용이 달라질 수도 있다. 기존 논문에서는 Context에 대한 처리과정에 대하여 언급하지 않고 있어 사용자의 상황에 맞게 콘텐츠를 가공할 수 없다.

② 사용자의 프라이버시 문제를 고려하지 않음

기존 논문은 사용자의 라이센스 취득과 인증 과정에서 사용자의 정보를 어떻게 보호할 것인가에 대해서는 논하지 않고 있다. 사용자의 데이터에 대한 접근 제어와 같은 방식으로는 DRM시스템을 효율적으로 운영하기 어렵다. 라이센스 취득과 사용자에 대한 인증 과정에서 사용자의 개인정보가 요구된다. 따라서 사용자의 익명성을 기반으로 한 사용자 데이터의 공개가 필요하다.

2.2. 웹서비스 기반의 DRM[2]

(1) HKUST의 DRM 시스템

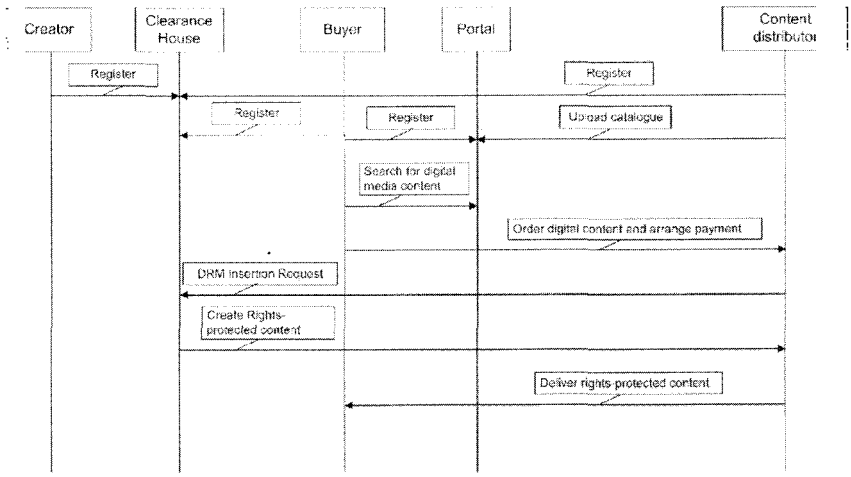
HKUST의 Sai Ho Kwok은 워터마크 기술을 기반으로 한 웹서비스 DRM 시스템을 제안하였다. 웹서비스 기술은 어플리케이션 통합의 새로운 아키텍처를 제공한다. 웹서비스 아키텍처에 의해 제공되는 유연성으로 입출력이 표준화된 시스템을 구성할 수 있다. 이러한 특징은 웹 어플리케이션을 위한 비즈니스 프로세스의 실현에 용이하다. 해당 연구는 웹서비스에 DRM을 적용해 보고 웹서비스 상에서의 워터마크 기반 DRM 시스템을 설계하였다. 제안한 방법은 시스템 간 동질성과 상호 운용성을 가질 수 있게 하고, 정보에 대한 보안과 프라이버시를 더욱 강화할 수 있으며 비즈니스에서의 프로세스를 최소화할 수 있다. 이러한 방법으로 전자상거래에서의 DRM에 대한 단점을 극복할 수 있다.

(2) 웹서비스를 이용한 워터마크의 삽입

저작권의 삽입은 일반적인 SOAP 프로토콜 내의 XML 메시지 교환을 행함으로써 웹서비스에 적용할 수 있다. <그림 3>은 온라인 미디어에 대한 분배 과정에서의 저작권에 대한 삽입을 가능하게 하는 각 개체 간 메시지 교환을 나타낸다. 각 절차 이전에 콘텐츠 제작자 및 판매자와 구매자는 상호 신뢰 관계에 있는 제3의 개체인 Clearance house가 필요하다. 이것은 그들의 개인 식별 정보 및 기타 정보 (예를 들어, 은행 계정 정보)를 가지고 있다. 개인 식별 정보는 워터마킹 절차에서 주요하게 사용된다. 예를 들어 은행 계정 정보는 지불에 사용하게 될 것이다. 저작권 관리 데이터베이스(RMDB:Rights Management Database)에서는 이러한 정보를 포함하고 있다. 저작권 서버(RMS:Rights Management Server)는 Clearance house 내에 존재한다.

구매자는 먼저 등록 절차가 필요하다. 디지털 미디어에 대한 항목을 선택 후 구매자는 콘텐츠 판매자를 지목한다. 그 이후 콘텐츠 판매자는 저작권이 보호된 미디어 콘텐츠를 준비하며 Clearance house는 저작권 관리 절차를 거치게 된다. 저작권이 보호된 콘텐츠가 준비되면, Clearance house는 콘텐츠 판매자에게 해당 콘텐츠를 양도한다.

저작권에 대한 삽입 절차는 <그림 3>과 같



〈그림 3〉 저작권 삽입을 위한 메시지 교환

이 나타날 수 있다. DRM 기술 제공자는 그들의 DRM제품을 UDDI내의 서비스 레지스트리에 등록할 것이다. Clearance house는 적절한 저작권 삽입 절차를 선택할 것이고 저작권 삽입에 관련된 기술 에 대한 정보를 제공할 것이다.

2.3. DRM 시스템에서의 프라이버시 보호[1]

(1) 개요

네덜란드의 필립스 연구소에서는 신원 기반의 DRM 시스템에 대한 문제점을 지적하고 이에 대한 프라이버시 대책을 제안하였다. 해당 연구에서는 디지털 오디오 및 비디오에 대한 내용의 배포에 있어서 발생되는 프라이버시 문제에 중점을 두고 사용자가 언제 어디에서든지 콘텐츠에 접근하는 것을 가능하게 하고 어떠한 장치에도 콘텐츠 제공자에 의해 발행된 증명서를 통하여 접근할 수 있게 한다.

DRM시스템이 사용자에 대한 권한을 설정하기 위해서는 사용자의 신원 정보를 필요로 한다. 이러한 사용자의 식별을 위해 스마트 카드를 사용한다. 스마트 카드는 인증 프로토콜을 작동하기 위해 하나의 공개키(PK)와 그에 대응하는 비밀 키(SK)를 가지고 있다.

사용자의 권리(UR:User Right)를 취득하기 위하여 다음과 같은 식별자를 보내게 된다.

UR = {c_id, r_d, PK}signCP

여기에서 c_id는 사용자가 접근하고자 하는 콘텐츠에 대한 식별자이다. r_d는 권리에 대한 속성 데이터이며 사용자가 콘텐츠에 대한 권리를 가지고 있다는 것을 의미한다. PK는 공개키이며 사용자에 대한 식별을 가능하게 한다. signCP는 콘텐츠 제공자(Contents Provider)의 서명을 나타낸다.

사용자에게 콘텐츠에 대한 접근을 승인하기 위한 시스템 작동 절차는 〈그림 4〉와 같다.

사용자가 콘텐츠를 이용하고자 할 때 그는 장치로부터 그 자신을 식별하고 그가 어떤 콘텐츠를 원하는지 장치에게 알려준다. 장치는 PK와 c_id의 취득 이후 사용자가 여기에 대한 사용 권한이 있는지에 대해 조사한다. 이러한 과정 이후에 사용자는 콘텐츠에 접근할 수 있게 된다.

(2) 프라이버시 문제

이러한 과정에서 다음과 같은 프라이버시 문제가 존재한다.

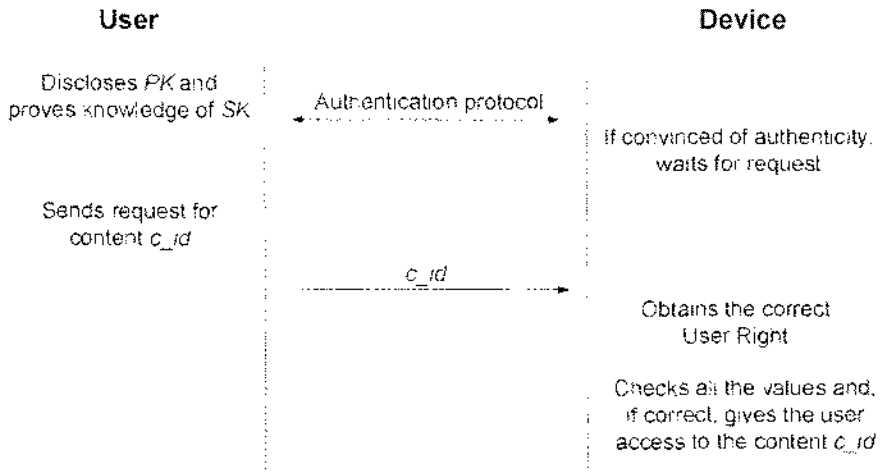
- 공개 키는 사용자의 유일한 식별자이다. 키가 사용자를 인증하기 위해 사용되어졌을 때 부터 공개키에 대한 노출의 위험성이 존재한다.
- 공개 키가 노출된 상태에서 그 공개 키를 통하여 네트워크를 검색함으로써 사용자의 권리에 대한 정보가 노출이 될 수 있다.
- 콘텐츠에 접근하는 동안 제 3의 인물이 사용자와 장치 사이에 sniffing공격을 통하여 사용자의 신원 정보를 취득함으로써 사용자에 대한 콘텐츠 사용 내역이나 사용자의 위치를 획득할 수 있다.

(3) PK의 보호

따라서 해당 연구에서는 사용자 권리(UR)의 전달 과정에서 PK를 보호하는 방법으로 다음과 같은 방법을 제안하고 있다.

$$UR - Ic\_id.H(PK.RAN).RAN)SignCP$$

이러한 방법으로 PK를 임의의 숫자 RAN을 통하여 해쉬함수를 거침으로 UR을 안전하게 전달할 수 있다. PK는 직접적으로 노출이 되지 않으며 설사 전송 과정의 모든 값을 획득한다고 하더라도 일방향 함수의 특성상 PK를 계산해 낼 수 없다.

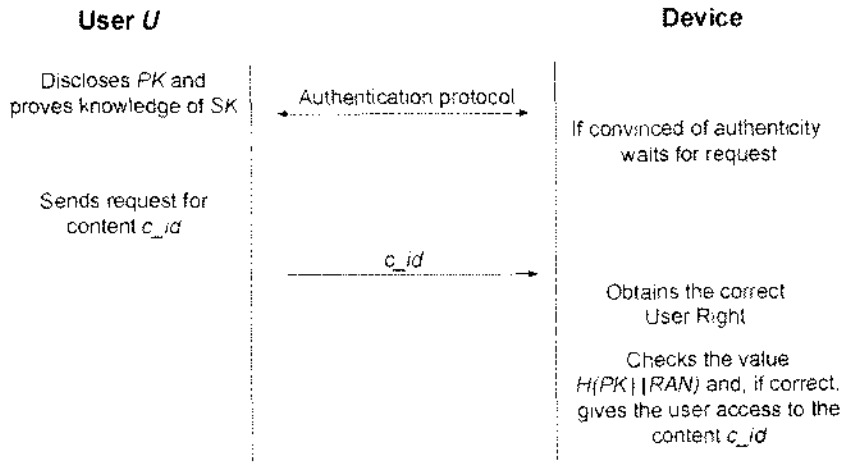


〈그림 4〉 User Rights를 확인하는 프로토콜

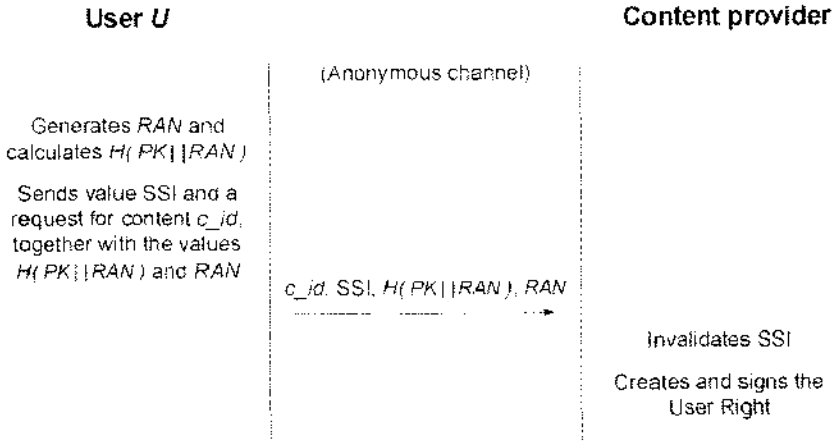
이러한 과정을 그림으로 나타내면 〈그림 5〉와 같다.

(4) 익명성을 보장하는 User Rights

익명성을 유지한 채로 User Rights를 획득하는 방안은 〈그림 6〉과 같다. 이 방법에서는 사용자가 대금 결제 이후 특정한 토큰(SSI:Secret Security Identifier)을 지급받고 그러한 SSI를 c_id, H(PK||RAN), 및 사용자에 의해 임의로 계산된 RAN과 함께 콘텐츠 제공자에 전송한다. 이러한 경우 콘텐츠 제공자는 사용자의 대금 결제 정보는 알 수 있으나 사용자에 대한 고유한 식별자는 알 수



〈그림 5〉 기밀성을 유지하는 User Rights 확인 프로토콜



〈그림 6〉 익명성을 유지한 User Rights 발급

없다. 따라서 이러한 방법으로 사용자에 대한 익명성을 지킬수 있다.

그러나 해당 연구는 다음과 같은 단점을 가지고 있다. 만약 전송 과정에서 전달되는 H(PK|RAN)과 RAN값이 악의를 가진 자에게 노출될 경우, 공격자는 다음 로그인 시에 이러한 값들을 이용하여 UR을 취득하고 콘텐츠에 대한 부정한 사용이 가능할 것이다. 따라서 이러한 방법은 Sniffing/Replay 공격에 취약하다. 제안한 방법은 Sniffing/Replay 공격에 안전한 OTP 메커니즘을 사용하였다. 따라서 악의를 가진 자로부터 원천적으로 사용자의 PK와 함께 인증 정보를 보호할 수 있다.

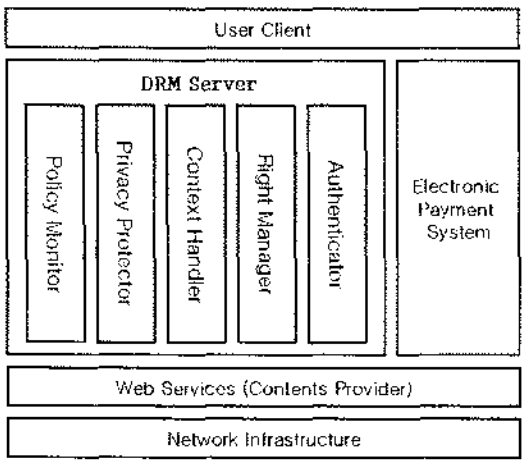
3. PADRM 아키텍처 설계

3.1. PADRM Architecture

본 논문의 Privacy Aware 특성을 갖는 DRM인 PADRM Architecture는 〈그림 7〉과 같다. 특정 콘텐츠는 웹서비스에 포함되어 있으며 DRM 시스템은 클라이언트 어플리케이션과 콘텐츠 제공자를 중재한다. DRM 시스템은 각각 사용자 인증, 저작권 관리, Context 취급, 프라이버시 보호, 프라이버시 정책 모니터로 구성되어 있다. Privacy Protector는 사용자의 Context를 수집하고 사용자의 동의를 얻은 정보의 경우에 한하여 Contents Provider에 전달한다.

DRM 서버 내 각 모듈의 기능은 다음과 같다.

- Authenticator : 사용자와 콘텐츠 제공자 간 인증에 대한 중재 역할을 한다.
- Right Manager : 콘텐츠 제작자의 저작권을 관리하고 디지털 콘텐츠를 발행한다.
- Context Handler : Context 정보에 대한 수집 및 가공 처리를 담당한다.



〈그림 7〉 PADRM Architecture

- Privacy Protector : Context Handler와 연동하여 사용자의 프라이버시 보호를 담당한다.
- Policy Monitor : 프라이버시 보호 정책을 모니터링한다.

3.2. 세부 설계

본 절에서는 콘텐츠 제작자가 콘텐츠를 등록하는 절차 및 최초 사용자와 콘텐츠 제공자 간에 인증 정보를 확립하는 방법과 인증에 필요한 절차들에 대하여 기술한다.

본 장에서 사용되는 기호들은 [표 1]과 같다.

3.2.1. 콘텐츠 등록

콘텐츠 등록은 저작권자와 콘텐츠 제공자 간의 특정한 정보 교환으로 이루어진다. 이 과정에서 저작권자 및 콘텐츠에 관한 정보를 확립할 수 있다. 콘텐츠 등록에 필요한 모듈은 [그림 8]과 같다.

각 모듈의 기능은 다음과 같다.

- Author Identifier : 저작권자를 식별하며 저작권자 정보를 데이터베이스에 기록한다.
- Contents Identifier : 콘텐츠 식별자 정보를 통제하고 요금 등 콘텐츠에 관한 정보를 데이터베이스에 기록한다.
- XrML Packager : 콘텐츠와 XrML 문서를 패키지한다.
- Contents Publisher : 패키지된 디지털 콘텐츠를 콘텐츠 제공자에게 전송한다.

각 절차에 따른 순차도는 〈그림 9〉에 나타나 있다.

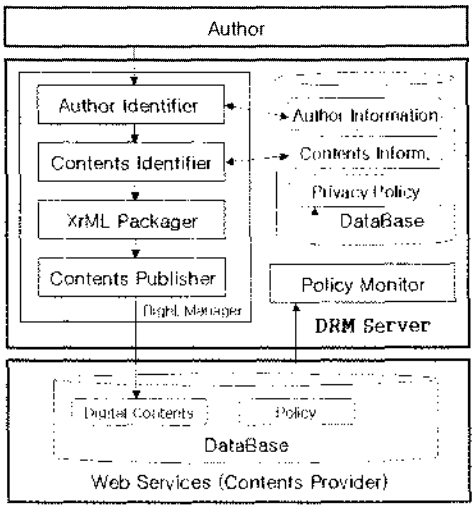
콘텐츠 등록 절차는 다음과 같다.

① 콘텐츠 제작자는 DRM 서버에 콘텐츠 발행을 요청한다.

② DRM 서버는 적절한 콘텐츠 식별번호

〈표 1〉 기 호

기호	의 미
OTP	일회용 패스워드
SEED	OTP의 생성원
||	합성 연산자
H(Str)Key	Str을 Key로 해쉬연산
E(Str)Key	Str를 Key로 암호화
D(Str)Key	Str를 Key로 복호화
TID	사용자 식별번호
SEQ	Sequence Number
PK	사용자의 공개키



〈그림 8〉 콘텐츠 등록

를 선택한다.

③ DRM 서버는 콘텐츠 제작자에게 콘텐츠 식별자를 전달한다.

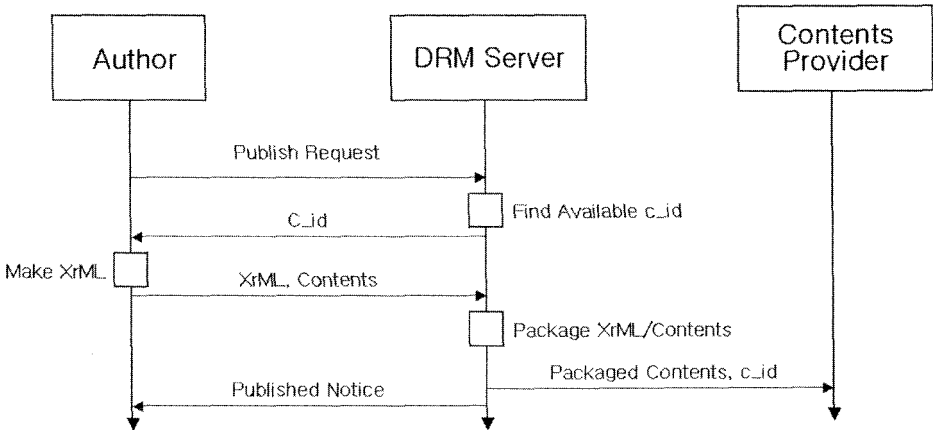
④ 콘텐츠 제작자는 저작권 정보를 XrML로 기술한다.

⑤ 콘텐츠 제작자는 DRM 서버에게 XrML 문서와 콘텐츠를 전달한다.

⑥ DRM 서버는 XrML과 콘텐츠 정보를 패키지한다.

⑦ DRM 서버는 패키지된 콘텐츠와 콘텐츠 식별번호를 콘텐츠 제공자에게 전달한다.

⑧ DRM 서버는 콘텐츠 제작자에게 발행이 끝났음을 알린다.



〈그림 9〉 콘텐츠 등록 절차

3.2.2. 라이센스 발급과 인증

라이센스 발급과 인증은 사용자와 콘텐츠 제공자 및 DRM 서버에 대한 상호작용으로 이루어진다. DRM Server는 사용자와 콘텐츠 제공자를 중재하며 콘텐츠 제공자에게는 사용자의 Context 및 콘텐츠에 대한 암호키를 제공한다. 사용자에 대한 라이센스를 발급 및 인증과 암호화에 필요한 필요한 모듈은 〈그림 10〉과 같다.

각 모듈의 기능은 다음과 같다.

① Contents Provider

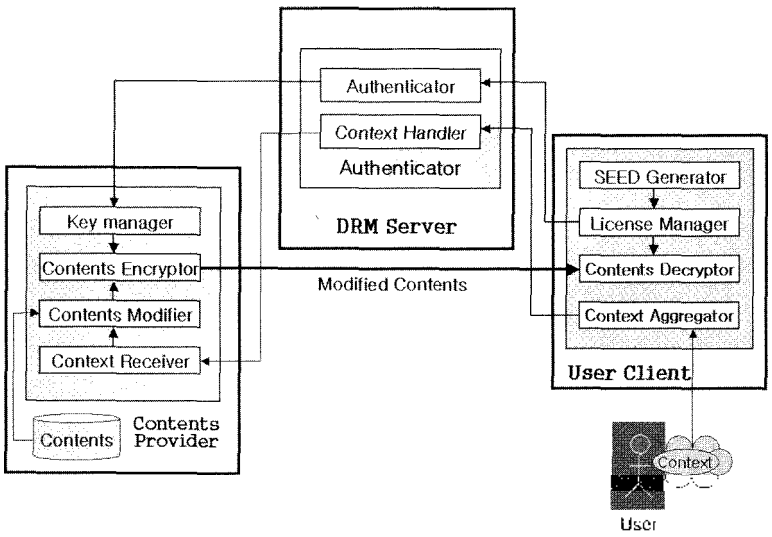
Key Manager : 콘텐츠 암호화에 사용될 키를 DRM서버 내의 인증 정보로부터 획득한다.

- Contents Encryptor : Key Manager를 통하여 획득한 키로 디지털 콘텐츠를 암호화한다.
- Contents Modifier : 디지털 콘텐츠를 취득하고 수신된 Context에 따라 가공 처리한다.

Context Receiver : DRM Server로부터 사용자의 Context를 획득한다. 이 경우는 프라이버시 정책에 위배되는 Context 정보는 전달되지 않는다.

② User Client

- SEED Generator : 사용자의 OTP를 생성하기 위한 SEED를 발생시킨다.
- License Manager : 라이센스 취득 절차에 따라 라이센스를 획득한다. 제안한 일련의 라이센스 취득 과정은 User Client의 License Manager와 DRM Server의 Authenticator의 상호작용으로 이루어진다.
- Contents Decryptor : 콘텐츠를 수신하고 복호화하여 사용자에게 전달한다.
- Context Aggregator : 사용자의 Context를 수신하고 DRM Server내의 Context



〈그림 10〉 사용자 인증 및 콘텐츠 암호화 모듈

Handler에 전송한다.

③ DRM Server

- Authenticator : 사용자의 인증 정보를 담당하고 라이센스를 발급하는 기능을 갖는다.
- Context Handler : 사용자의 Context를 수집하고 가공 처리하여 Contents Provider로 전송한다.

(1) 라이센스 발급 절차

라이센스 발급 단계는 User Client가 DRM 서버를 통하여 콘텐츠에 접근할 수 있는 권한을 부여하는 단계이며 이 과정에서 상호간 TID, OTP, SEED가 보관된다. 라이센스를 발급하는 단계는 다음과 같다. 먼저 사용자는 DRM 서버에게 콘텐츠의 식별자인 c_id와 함께 $H(H(PK)^{SEED}||SEED)$를 OTP로 전송한다. DRM 서버는 H(OTP||RAN)를 TID로 하여 XrML과 함께 사용자에게 제공한다. 사용자는 여기에서 발급된 TID를 통하여 자신의 Identity를 확립할 수 있다. 이후 사용자는 자신의 TID를 밝힌 후 지불 시스템에 지불을 한다. 지불 시스템은 지불의 확인 후 DRM 서버에게 지불이 완료된 TID를 제공한다. 이러한 과정을 순차도로 표현하면 〈그림 11〉과 같다.

① 사용자는 DRM 서버에게 콘텐츠 식별자와 인증 정보를 전달한다.

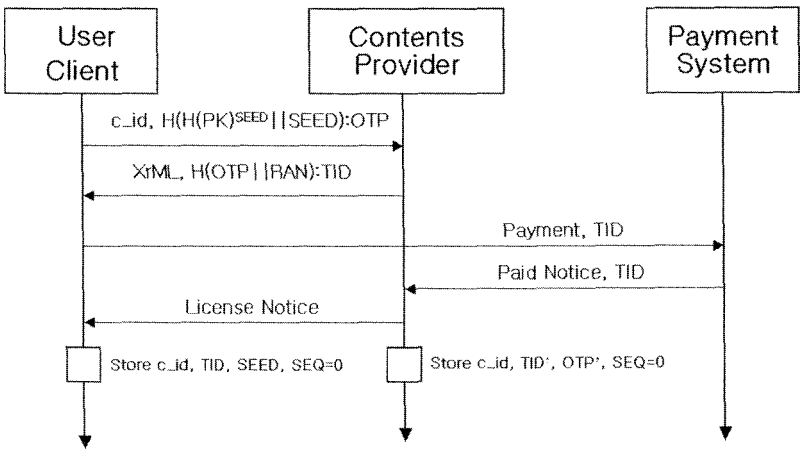
② DRM 서버는 사용자에게 XrML문서와 임시 아이디를 전달한다.

③ 사용자는 지불시스템을 통하여 콘텐츠 사용료를 지불한다.

④ 지불 시스템은 결제가 끝난 후 DRM 서버에게 지불이 완료되었음을 알린다.

⑤ DRM 서버는 사용자에게 라이센스 취득 절차가 끝났음을 알린다.

⑥ 사용자와 DRM 서버는 각 파라미터를 저장한다.



〈그림 11〉 라이센스 발급 절차

(2) 인증 및 콘텐츠 암호화 절차

인증 단계는 사용자가 DRM 서버에 자신의 식별자와 함께 라이센스를 전달하여 DRM 서버가 사용자를 인증하고 콘텐츠의 접근 권한을 확인하는 단계이다. 사용자를 인증하는 단계는 다음과 같다. 먼저 사용자는 DRM 서버에게 콘텐츠의 식별자인 c_id와 함께 앞서 저장된 TID, SEED, 그리고 사용자 고유의 비밀 키인 PK를 SEED로 해쉬연산을 하여 전달한다. 이후 DRM 서버는 현재 사용자가 전송한 SEED와 $H(PK)^{SEED}$에 대한 해쉬연산을 거친 후 앞서 저장한 OTP와 일치하는가를 확인한다. 사용자가 확인되면 새로운 OTP를 요청하게 되고 사용자는 $H(H(PK)^{SEED'}||SEED')$를 연산하여 그 결과값을 DRM 서버에게 새로운 OTP로 전달하게 된다. 이후 DRM 서버는 OTP'를 저장하고 임의의 숫자인 RAN을 계산한다. 이후 DRM 서버는 OTP'||RAN'에 대한 해쉬연산을 거치고 사용자에게 이 값을 TID로 전달한다. 이 경우 사용자는 다음의 접속 시에 TID로 자신의 Identity를 확인할수 있을 것이다. 이러한 과정은 〈그림 12〉와 같다.

① 사용자는 DRM 서버에게 인증 정보를 전달한다.

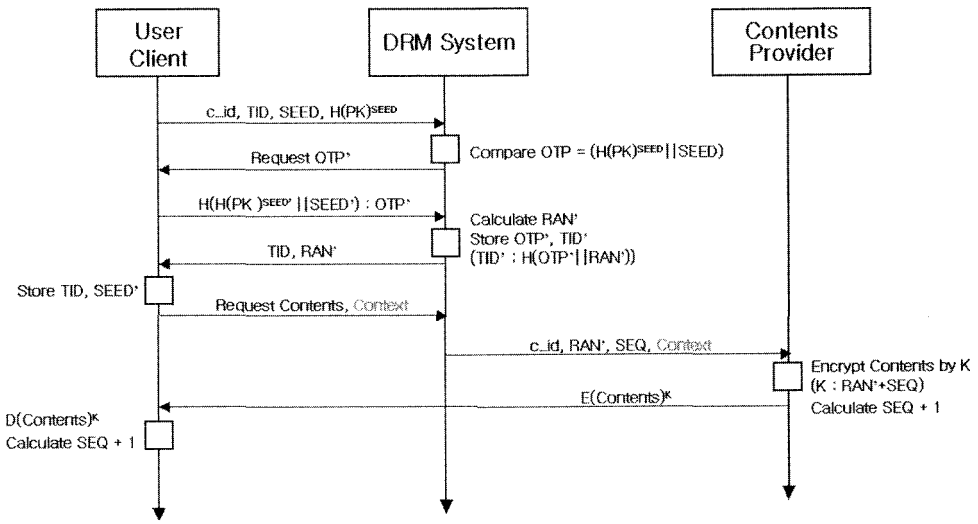
② DRM 서버는 미리 저장된 OTP와 인증 정보에 대한 연산이 일치하는지를 확인한다.

③ DRM 서버는 확인 후 새로운 OTP를 요청한다.

④ 사용자는 새로운 OTP'를 계산하여 전송한다. (여기에서 라이센스는 SEED가 된다.)

⑤ OTP와 TID를 계산 후 저장하고 임의의 숫자를 생성 후 TID와 함께 사용자에게 전송한다.

⑥ 사용자는 TID와 SEED를 저장한다.



〈그림 12〉 인증 및 콘텐츠 암호화 절차

⑦ 사용자는 콘텐츠를 요청한다.
⑧ DRM 서버는 콘텐츠를 미리 계산하였던 RAN'과 SEQ를 합하여 키로 하고 콘텐츠를 암호화한다.
⑨ 사용자는 암호화된 콘텐츠를 RAN'과 SEQ로 복호화한다.

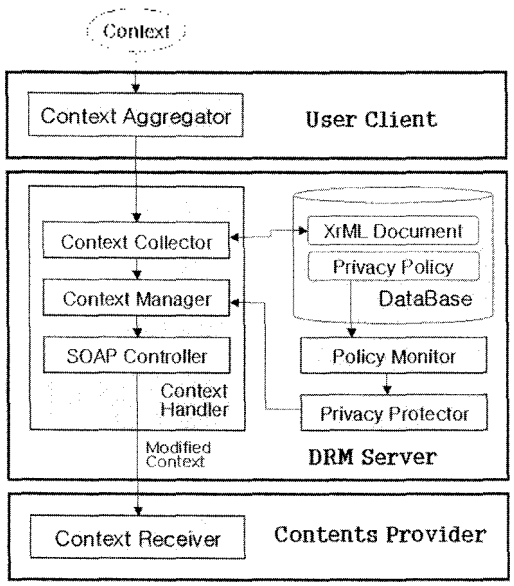
3.2.3. 저작권 정보 및 Context의 전달

(1) 프라이버시를 고려한 Context의 전달

Context는 기본적으로 프라이버시를 고려하여 전달된다. Context Handler 내의 Context Collector는 XrML의 Context 요구사항에 따라 Context를 수집하고 Context Manager에 전달한다. Policy Monitor는 프라이버시 정책을 모니터링하고 Privacy Protector는 이를 기반으로 Context Manager 내에 있는 Context 정보를 가공한다. SOAP Controller는 가공된 Context 정보를 SOAP 메시지 내에 삽입한다. 이렇게 가공된 Context를 포함한 SOAP 메시지가 콘텐츠 제공자에게 전달되며 콘텐츠 제공자는 이를 근거로 디지털 콘텐츠에 Context 정보를 반영할 수 있다. 프라이버시 문제를 고려한 Context의 전달 과정은 〈그림 13〉과 같다.

각 모듈의 기능은 다음과 같다.

- Context Collector : User Client의 Context Aggregator로부터 사용자의 Context 정보를 수집한다.
- Context Manager : Privacy Protector와 연동하여 Context 에 대한 가공 절차를 거친다.
- SOAP Controller : 가공된 Context정보를 SOAP 메시지 내에 삽입함으로써



〈그림 13〉 프라이버시를 고려한 Context의 전달과정

Contents Provider에 대한 Context 전달을 용이하게 한다.

- Policy Monitor : 사용자의 프라이버시 보호를 위한 정책을 가져온다.
- Privacy Protector : Policy에 맞게 사용자의 Context에 대한 공개 여부를 판단하고 Context Manager와 연동하여 Context 정보를 가공 처리한다.

(2) Context를 고려한 XrML 스키마

전형적인 XrML문서의 구조는 <그림 14>와 같다.[11]

```
<XrML>
    <BODY>
        (ISSUED)
        (TIME)
        (DESCRIPTOR)
        (ISSUER)
        (ISSUEDPRINCIPALS)
        (WORK)
        (AUTHENTICATEDDATA)
    </BODY>
    (SIGNATURE)
</XrML>
```

<그림 14> 전형적인 XrML 문서 구조

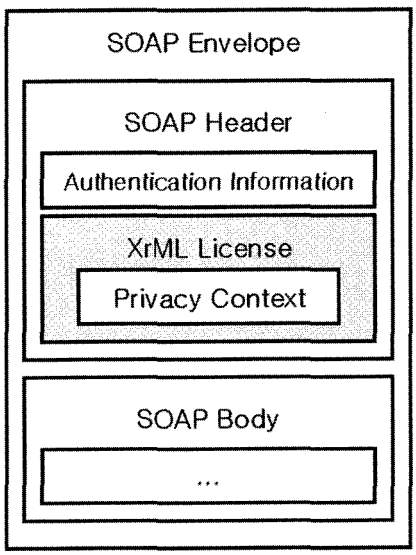
저작권 기술에 필요한 사항을 XrML 문서에서 나타내고 있다. <BODY>이내에 기록되는 사항은 필수사항이며 (SIGNATURE)는 선택사항으로 되어 있다. 그러나 XrML문서는 콘텐츠 가공에 필요한 Context 정보를 기록할 수 없다. 따라서 본 논문에서는 XrML 문서 내에 <PrivacyContext>엘리먼트를 추가하여 콘텐츠 제공에 필요한 Context 정보에 대해 기술하는 방법을 제안한다. 제안하는 XrML 스키마는 <그림 15>와 같다.

```
<XrML>
    <BODY>
        (ISSUED)
        (TIME)
        (DESCRIPTOR)
        (ISSUER)
        (ISSUEDPRINCIPALS)
        (WORK)
        (AUTHENTICATEDDATA)
        (PRIVACYCONTEXT)
    </BODY>
    (SIGNATURE)
</XrML>
```

<그림 15> 변형된 XrML 문서 구조

(3) SOAP를 통한 라이센스 및 Context 전달

XrML 라이센스를 포함한 SOAP메시지는 <그림 16>에 나타나 있다. 그림에서 SOAP메



<그림 16> 라이센스가 포함된 SOAP

시지 내에 XrML 라이센스와 함께 사용자의 Privacy Context가 첨부된 것을 알 수 있다.[13] SOAP에 Context를 첨부하는 과정은 Context Handler 내의 SOAP Controller에서 이루어진다.

라이센스가 포함된 XML문서는 <그림 17>과 같다. XrML라이센스는 SOAP Header내에 포함되며 이러한 라이센스 정보를 통하여 콘텐츠에 접근할 수 있다. 아래는 토큰을 포함한 라이센스를 SOAP Header 내에 첨부한 경우를 나타내고 있다.[8]

```
<S:Envelope xmlns:S="...">
   <S:Header>
      <wsse:Security xmlns:wsse="...">
         <xrml:license xmlns:xrml="..."
                       licenseId="urn:SecurityToken-ef375268"/>
            ...
            <PrivacyContext>
              <Location>
                 <address keyName="City" keyValue="40">
                  KB-235-7340 Seoul</address>
              </Location>
              <Client>
                 <DeviceDefaults>PDA</DeviceDefaults>
                 <Hardware>
                    <ScreenSize>320x200</ScreenSize>
                    <IsColorCapable>Yes</IsColorCapable>
                 </Hardware>
              </Client>
            </PrivacyContext>
         </xrml:license>
         <ds:Signature xmlns:ds="...">
            ...
            <ds:KeyInfo>
              <wsse:SecurityTokenReference>
                <wsse:Reference URI="urn:SecurityToken-ef375268"
                               xmltok:RefType="xrml:license"
                               xmlns:xmltok="..."/>
```

<그림 17> XrML 라이센스가 포함된 XML문서

4. 분 석

4.1. PADRM 시스템 요구사항 분석

PADRM 시스템을 설계하기 위해서는 몇 가지 특성이 요구된다. 본 절에서는 이러한 요구사항에 대하여 기술한다.

(1) Context-Aware 환경에 대한 고려

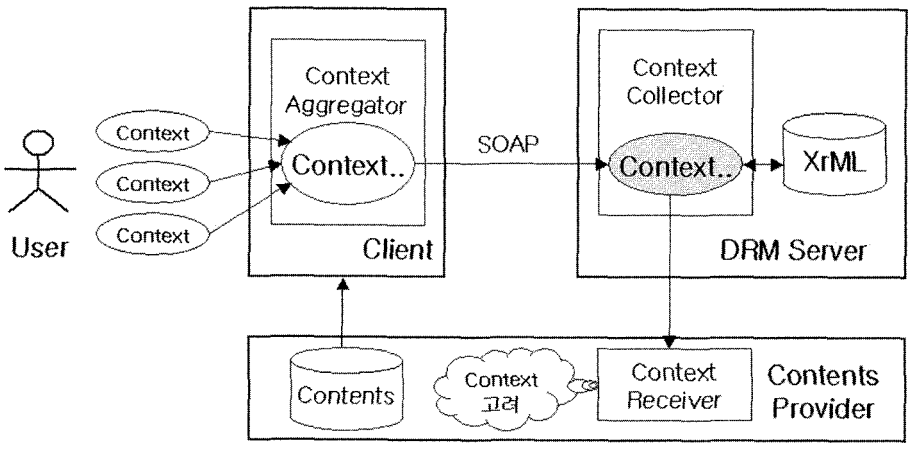
전통적으로 DRM 시스템 구조는 비교적 정적인 요구사항을 가정한다. 콘텐츠에 대한 접근제어 결정은 사용자의 Context에 따라 변화하거나 환경조건의 상황에 따라 변화하지 않기 때문이다. 그러나 유비쿼터스 환경에서 사용자에게 적절한 콘텐츠를 제공하기 위해서는 Context에 대한 고려가 필요하다. Context를 고려한 동적인 구조는 사용자의 상황에 따른 가장 적합한 콘텐츠를 제공할 수 있다.

PADRM에서는 사용자의 Context를 클라이언트의 Aggregator에서 수집하고 DRM 서버의 Context Collector로 전달한다. PADRM에서의 Context의 전달 과정이 〈그림 18〉에 나타나 있다.

(2) 익명성 보장

콘텐츠 제공을 위하여 사용자에 대한 정보가 적절히 공개되어야 한다. 그러나 사용자의 정보에 대한 공개는 프라이버시의 침해로 이어질 수 있다. PADRM시스템은 OTP를 이용하여 사용자 개인의 신원을 밝히지 않은 상태에서 라이센스를 획득할 수 있으므로 익명성을 보장할 수 있다. 본 논문에서는 필립스 연구소가 제안한 알고리즘을 개선한 일회용 패스워드 방식의 인증 방법을 제안한다. 일회용 패스워드는 한 번 이상 사용되지 않으므로 사용자에 대한 익명성을 보장할 수 있다.

익명성의 보장을 위해서 먼저 사용자에 대한 라이센스 발급 절차와 함께 사용자의 콘텐



〈그림 18〉 PADRM의 Context 전달과정

츠 접근 시 인증하고 라이센스를 확인할수 있는 절차가 필요하다. 아래는 이러한 절차에 대하여 살펴본다.

1) 익명을 고려한 라이센스 발급

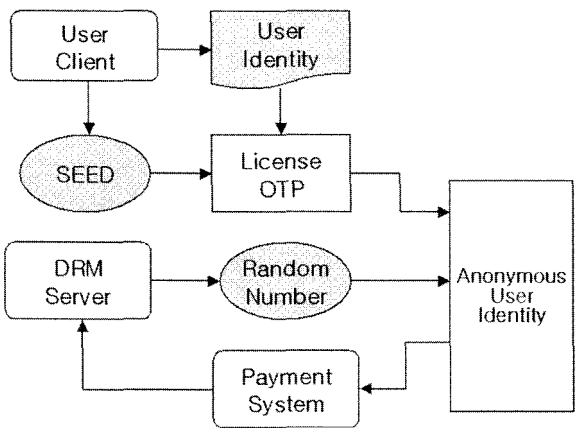
라이센스 발급은 사용자와 콘텐츠 제공자 간 익명 아이디와 라이센스 토큰인 OTP를 확립하는 단계이다. 발급 절차는 〈그림 19〉와 같다.

사용자 클라이언트는 SEED를 생성한 후 이를 기반으로 라이센스 토큰으로 사용될 수 있는 OTP를 생성한다. 한편, DRM 서버는 적절한 임의의 숫자를 생성한다. 이러한 과정에서 생성된 OTP와 Random Number에 대한 해쉬연산을 거침으로써 사용자 익명 아이디를 발급한다. 사용자는 이러한 익명 아이디를 제시하고 대금을 지불하며 지불 시스템은 정당한 금액의 지불 확인 후 콘텐츠 제공자에게 해당 익명 아이디에 대한 대금 지급이 완료되었음을 통보한다. 이러한 과정 중에서 사용자의 SEED 및 DRM 서버의 Random Number는 노출되지 않았다. 따라서 사용자는 다음 인증 과정에서 SEED를 제시하면 사용자 본인임을 확인할 수 있을 것이다.

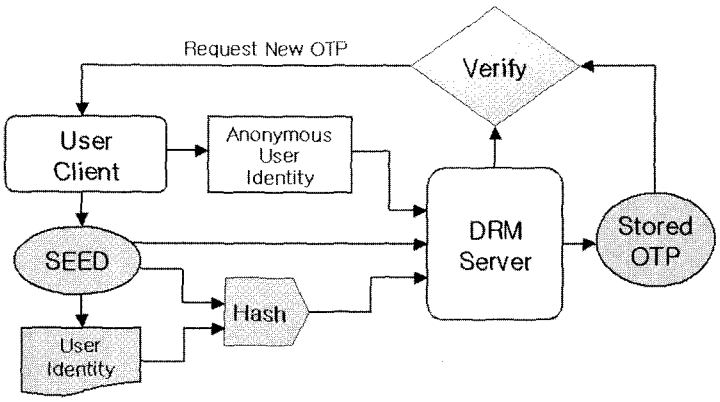
2) 익명을 고려한 인증

인증 단계는 사용자가 DRM 서버에 자신의 식별자와 함께 라이센스를 전달하여 사용자를 인증하고 콘텐츠의 접근 권한을 확인하는 단계이다. 인증 알고리즘은 〈그림 20〉과 같다.

사용자 클라이언트는 라이센스 발급 과정에서 부여받은 익명 아이디를 DRM 서버에 전달한다. 또한, OTP 발급에 사용되었던 SEED와 함께 사용자의 Identity와 SEED에 대한 Hash 연산의 출력을 DRM 서버에 전달한다. DRM 서버는 앞서 저장된 OTP와 현재의 인자들의 연산을 비교하여 같은지를 검증한다. 검증 결과 사용자가 인증되면 새로운 OTP를 요청하게 된다. 이 경우 사용자의 Identity는 노출되지 않았다. 따라서 사용자는 익명을 유지한 상태에서 안전하게 DRM 서버에게 본인



〈그림 19〉 OTP와 익명 아이디 발급 절차



〈그림 20〉 사용자 인증 절차

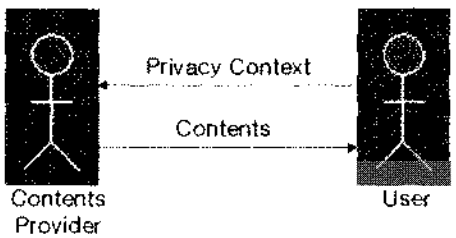
의 Context를 제공할 수 있게 된다.

(2) Dynamic한 콘텐츠 접근

한 번의 라이센스 취득 후 유효기간동안 사용자는 언제, 어디서 어떤 장비를 사용하여도 콘텐츠에 접근할 수 있어야 한다. 한편, 콘텐츠 제공자는 다양하게 접근하는 사용자를 식별할수 있어야 한다. 제안한 시스템은 스마트 카드와 같은 별도의 저장 장치만 소지하고 있으면 언제 어디서든 라이센스를 취득한 콘텐츠에 접근이 가능하다. 본 논문에서의 라이센스 취득 방법은 시간과 공간 및 장비에 대한 제약 없이 안전하게 사용자를 인증하고 라이센스를 취득할 수 있다. 따라서 사용자는 언제 어디서나 콘텐츠에 대한 접근이 가능하다. 이러한 콘텐츠 유통 과정에서 고려해야 할 사항은 다음과 같다.

1) 콘텐츠 유통 과정에서의 정보 전달

콘텐츠는 사용자의 상황에 따라 다르게 가공될 필요가 있다. 콘텐츠에 대한 제공은 사용자의 편의를 최대한 고려하여야 한다. 콘텐츠의 제공 방법은 사용자의 신원이나 현재 위치, 시간 등에 따라서도 달라질 것이다. 제안한 아키텍처는 사용자의 Context에 대하여 고려하고 있다. 콘텐츠의 적절한 제공을 위한 콘텐츠 유통 과정에서 정보의 흐름은 〈그림 21〉과 같다.



〈그림 21〉 콘텐츠 유통 과정에서의 정보 전달

① Privacy Context

Privacy Context는 사용자 개인을 식별할 수 있거나 노출시 악의적으로 이용될 가능성이 있는 Context이다. 따라서 Privacy Context에는 적절한 보호가 필요하다. 그러나 콘텐츠

제공자는 양질의 콘텐츠를 제공하기 위해 기본적으로 사용자의 Context가 필요하다. 또한 사용자의 상황에 따라 제공하고자 하는 콘텐츠의 종류나 범위가 달라질 수 있다. 사용자에게 맞게 가공된 콘텐츠의 전달을 위해서는 사용자의 Context가 필수적이다.

② Contents

콘텐츠는 사용자의 Context에 따라 현재 상황에 맞게 적절히 가공된다. 예를 들어, 콘텐츠 스트리밍 서비스의 경우 사용자의 장치가 데스크톱 PC인가 PDA인가에 따라서 서비스가 달라질 수 있을 것이다. 한편, 사용자가 청소년일 경우와 성인일 경우에 영화의 중간 부분이 삭제되는 경우도 생각해 볼 수 있다. 이렇게 사용자의 Context 정보 제공 이후 사용자의 취향이나 상황 및 장치에 맞게 가공된 콘텐츠를 전달받을 수 있다.

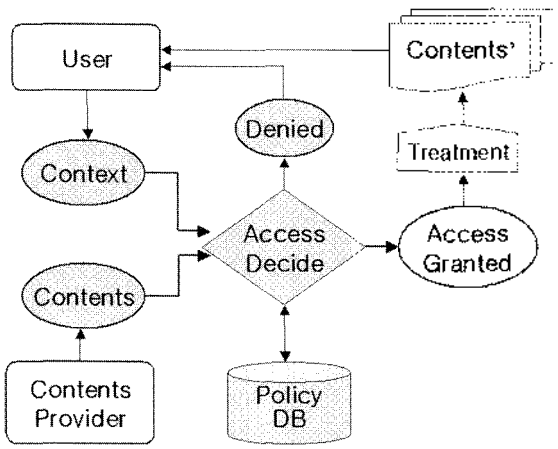
2) 콘텐츠의 가공

콘텐츠는 사용자의 상황에 맞게 가공되어야 하며 사용자의 Context가 요구된다. 원본 디지털 콘텐츠는 사용자의 Context에 따라 가공 과정을 거치고 새로운 콘텐츠를 생성한다. 사용자는 이렇게 현재 상황에 맞게 가공된 디지털 콘텐츠를 제공받을 수 있다. 한편, 특별한 사유에 의해 엑세스가 거부될 경우는 거부 메시지를 받게 된다. 디지털 콘텐츠의 공개 여부는 Policy DB에 의해 이루어진다. 디지털 콘텐츠가 가공되는 과정을 간단히 표시하면 〈그림 22〉와 같다.

3) 콘텐츠에 요구되는 Context 정보의 표현[12]

콘텐츠 제공에 필요한 Context 정보의 요청은 2가지 타입이 존재한다.

- **mandatory** : 서비스 제공에 필수적으로 필요한 데이터
- **optional** : 데이터를 선택적으로 제공할 수 있음



〈그림 22〉 콘텐츠의 가공 절차

Context 정보에 대한 기술은 DAML-S 언어를 사용한다. DAML-S는 웹서비스의 프레임워크를 확장하여 시맨틱 웹 기반의 기술을 적용하고 웹서비스를 기술할 수 있으며, 에이전트 기술을 중개에 활용할 수 있다. DAML-S는 시맨틱 웹서비스를 구현하기 위한 핵심적인 컴포넌트로 DARPA에 의해 개발된 DAML+OIL기반의 서비스 기술을 위한 온톨로지 언어이다. DAML-S는 SOAP, WSDL과 같은 산업계 표준들의 상위 수준에 구축되어 웹서비스의 탐색, 요청, 상호운용, 합성, 검증, 통제 등을 담당할 수 있으며 에이전트의 추론 기능과 애플리케이션을 사용한 서비스의 자동화된 상호 운용을 지원할 수 있다.[5]

제안한 아키텍처에서 특정 디지털 콘텐츠에 필요한 Privacy Context 정보 기술에 DAML-S가 사용되는 이유는 아래와 같다.

① Context에 의미를 부여할 수 있다.

웹서비스는 일종의 웹 자원이다. 그러나 DAML-S는 구체적인 의미에 대한 구조를 정의한다. Context는 의미를 가진 정보의 집합이다. 따라서 Context에 대한 의미를 정의하는데 DAML-S가 효율적으로 사용될 수 있다.

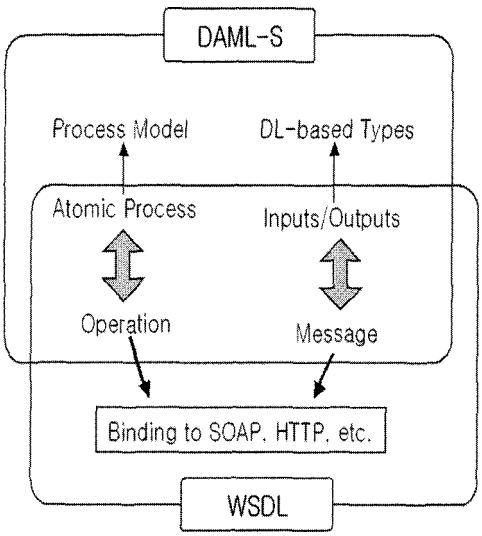
② 프라이버시를 고려한 Dynamic DRM 서비스 제공

Context의 의미를 컴퓨터가 이해할 수 있으므로 콘텐츠 제공자에게 필요한 Context만을 검색, 추론하고 이를 콘텐츠 제공자에 적절하게 재가공하여 사용자에게 콘텐츠를 적응적(Adaptive), 적시적(Just-in-Time)으로 제공할 수 있다. 이 과정에서 사용자의 프라이버시에 대한 침해를 받을 수 있는 Context는 원천적으로 전달되지 않는다. 따라서 프라이버시 문제를 고려한 Dynamic DRM 시스템 구축이 가능하다.

③ 웹서비스와 상호 보완적인 사용이 가능하다.[5]

DAML-S는 웹서비스의 WSDL과 유사한 기능을 갖고 있다. 그러나 DAML-S는 DAML+OIL 클래스에 정의된 데이터 형식과 XML스키마의 데이터형식을 사용할 수 있어 WSDL의 데이터 형식 메커니즘을 확장한 형태를 갖는다. 따라서 WSDL과 독립적으로 사용하고 SOAP에 함께 Binding할 수 있다. 또한 <그림 23>에 나타난 것과 같이 두 언어는 같은 공간을 포함하지 않도록 정의되었기 때문에 상호 보완적인 특성을 가질 수 있다.

DAML-S를 통한 Context 엘리먼트 요청에 대한 기술방법은 <그림 24>와 같다.[12]



<그림 23> DAML-S와 WSDL의 상호보완성

```
<rdf:Property rdf:ID="mandatory">
<rdfs:subPropertyOf rdf:resource="&process;
                                  #inputParameter"/>
</rdf:Property>
<rdf:Property rdf:ID="optional">
<rdfs:subPropertyOf rdf:resource="&process;
                                  #inputParameter"/>
</rdf:Property>
```

〈그림 24〉 DAML-S를 통한 데이터 엘리먼트 요청 기술

(3) 콘텐츠의 기밀성 유지

콘텐츠는 암호화된 상태에서 배포되어야 한다. 콘텐츠를 그대로 전달하는 것은 전송 과정에서 Sniffing 되어질 수 있다. 제안한 시스템은 세션마다 암호 키가 변화하므로 콘텐츠에 대한 기밀성을 보장할 수 있다.

본 시스템에서 사용자에게 제공되는 디지털 콘텐츠는 암호화 된 형태로 제공된다.

$$C' = E(C,R,S)$$

여기에서 C'는 암호화된 콘텐츠를 의미한다. R은 콘텐츠 제공자가 생성한 임의의 숫자이며 S는 라이센스가 발급된 이후로부터 진행된 순차적인 수열 가운데 하나이다. 키의 생성은 임의의 숫자와 함께 Sequence Number를 합산하여 생성한다.

따라서, 콘텐츠에 대한 암호화 방법은 아래와 같다.

$$\mathrm{Encrypt}(\mathrm{Contents})^{K},\quad K = R+S$$

암호화 알고리즘은 DES를 사용한다. 디지털 콘텐츠 암호화에 사용되는 키 R과 S의 합이다.

한편, 복호화의 방법은 다음과 같다.

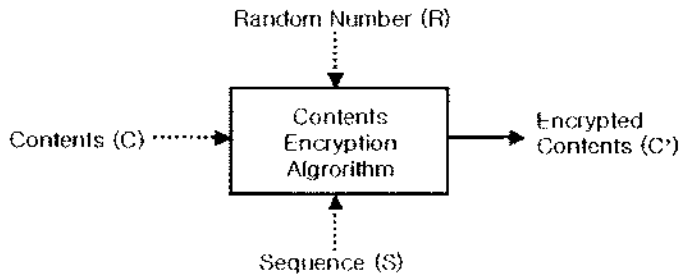
$$C = D(C',R,S)$$

C는 원본 콘텐츠를 의미한다. 클라이언트는 콘텐츠 전송 과정에서 임의의 숫자를 서버로부터 발급받게 되며 해당 Sequence Number를 합산하여 키를 생성할 수 있다. 암호화된 콘텐츠를 이러한 키로 복호화하면 원본 디지털 콘텐츠를 생성할수 있다.

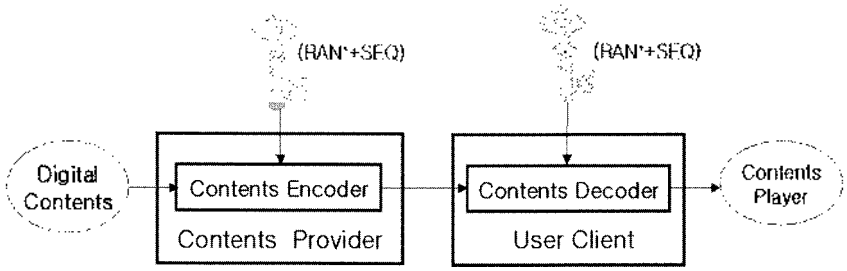
여기서 임의의 숫자는 매 세션마다 변화하며 Sequence Number는 세션마다 1씩 증가한다. 따라서 암호화에 쓰이는 키는 수시로 변화하며 설사 악의를 가진자가 암호화 키를 중간에 가로챈다고 하더라도 키 값은 한 번밖에 사용되지 않으므로 무의미하다.

콘텐츠에 대한 암호화 및 복호화 절차는 〈그림 26〉과 같다.

이 과정에서 콘텐츠 웹서비스와 사용자의 클라이언트는 각각 인증 과정에서 생성된 값을 통하여 암호화 키를 생성할수 있다. 한편,



〈그림 25〉 암호화 알고리즘



〈그림 26〉 키 생성 및 콘텐츠 전달

부정한 사용자가 콘텐츠 웹서비스에 접근하는 경우는 RAN' 값을 취득하지 못하므로 콘텐츠에 대한 복호화를 할 수 없다.

4.2. 요구사항에 따른 시스템 비교

Dynamic한 DRM의 요구사항에 따라 요약한 결과가 〈표 2〉에 나타나 있다.

HKUST와 Philips 시스템에서는 Context 환경에 대한 언급이 없다. 따라서 사용자의 상황을 고려한 DRM 서비스를 제공할 수 없다. PADRM은 각 클라이언트, DRM 서버, 콘텐츠 제공자의 환경에 Context에 대한 처리 모듈이 있으며 이를 통하여 사용자의 Context를 서비스 제공 환경에 반영할 수 있다. 한편, HKUST에서는 익명성에 관하여 언급하지 않고 있다. 따라서 익명에 따른 사용자의 프라이버시를 보호할 수 없다. Philips 시스템에서는 이를 위한 환경을 제공하고 있으며, 구체적인 발급 절차를 명시하고 있다. 그러나 Philips에서 제안한 알고리즘은 요청과 응답을 통한 메시지 교환이 이루어지는 웹서비스 환경을 고려하지 않고 있다. 따라서 웹서비스 환경에 적절한 파라미터 교환 방법이 필요하다. PADRM에서는 웹서비스 환경에서 사용자의 라이센스 발급과 인증을 익명으로 가능하게 한다. 따라서 사용자의 익명성을 통한 프라이버시를 보장할 수 있다. 한편,

〈표 2〉 요구사항에 따른 비교

	Context 환경 고려	익명성 보장	Dynamic 콘텐츠 접근	콘텐츠 기밀성 유지
HKUST	×	×	×	○
Philips	×	○	×	×
PADRM	○	○	○	○

* × : 고려하지 않음
* ○ : 고려하고 있음

HKUST와 Philips는 Context-Aware환경을 기반으로 설계되지 않았으므로 Dynamic하게 콘텐츠를 제공할 수 없다. PADRM에서는 구체적으로 Context 환경을 고려하여 설계되었으므로 이러한 문제를 해결할 수 있다. 또한 HKUST와 Philips에서는 콘텐츠 암호화에 필요한 키를 어떻게 분배할 것인가에 관한 문제를 언급하지 않고 있다. PADRM은 인증 단계의 각 파라미터의 전송 과정에서 사용자와 콘텐츠 제공자의 키를 생성할 수 있다.

4.3. 안전성 분석

본 절에서는 알려진 공격 기법을 중심으로 제안한 아키텍처의 안전성을 분석한다.

(1) Sniffing/Replay 공격

Philips 시스템은 사용자 권리(UR)의 전달 과정에서 사용자의 개인 식별자가 되는 공개키(PK)를 보호하는 방법으로 다음과 같은 방법을 제안하고 있다.

$UR=\{c\_id, H(PK||RAN), RAN\}_{signCP}$

이러한 방법으로 PK를 임의의 숫자 RAN을 통하여 해쉬함수를 거침으로 UR을 안전하게 전달할 수 있다. 이러한 경우 PK는 직접적으로 노출이 되지 않으며 전송 과정의 모든 값을 획득한다고 하더라도 일방향 함수의 특성상 PK를 계산해 낼 수 없다.

그러나 이러한 경우, 다음과 같은 문제점을 가지고 있다. 만약 전송 과정에서 전달되는 H(PK||RAN)과 RAN값이 악의를 가진 자에게 노출될 경우, 공격자는 다음 로그인 시에 이러한 값들을 이용하여 UR을 취득하고 콘텐츠에 대한 부정한 사용이 가능하다. 따라서, 사용자와 콘텐츠 제공자간에 전달되는 인자값에 대한 Sniffing 공격의 경우 사용자 고유의 식별자인 PK에 대한 보호만 가능하며 사용자의 권리인 UR은 보호할 수 없다.

제안한 방법은 이러한 점을 다음과 같은 방식으로 해결한다. 최초 라이센스 발급시 사용자는 DRM 서버에게 콘텐츠의 식별자인 c_id와 함께 $H(H(PK)^{SEED}||SEED)$를 OTP로 전송한다. DRM 서버는 OTP와 적절한 랜덤 숫자에 대한 해쉬값을 TID로 하여 사용자에게 제공한다. 이후에 사용자는 TID를 통하여 서

버로부터 인증받고 콘텐츠에 대한 사용 권리를 확인할 수 있다. 이러한 경우, 인증 과정에서 OTP를 새롭게 생성하며 TID의 값은 새로운 OTP에 따라 변경된다. 따라서 한 번 사용된 TID는 다시는 사용되지 않는다. 그러므로 PADRM 시스템은 사용자와 DRM 서버 간 전달되는 값에 대한 Sniffing/Replay 공격으로부터 안전하다.

(2) 서버 침해 공격

Philips 시스템에서는 콘텐츠에 대한 사용자의 권리를 식별하기 위해서 다음과 같은 인자값을 고려한다.

UR={c_id,H(PK||RAN),RAN}signCP

콘텐츠 제공자가 RAN으로부터 H(PK||RAN)를 검증하고, c_id값에 대하여 콘텐츠의 사용 권한을 확인하는 절차를 위해서는 사용자의 PK값이 필요하다. 따라서, 콘텐츠 제공자는 사용자의 개인 식별 정보를 저장하고 있어야 한다. 이러한 경우, 콘텐츠 제공자가 서버 침해 공격을 당할 경우 사용자의 개인 식별 정보로부터 사용자의 개인정보가 노출될 수 있다.

제안된 시스템은 사용자의 사용자가 전송한 $H(PK)^{SEED}$ 값과 SEED 값을 통하여 저장된 OTP값을 연산할수 있는지에 대한 확인 과정을 통하여 사용자를 인증한다. 서버에는 OTP와 TID만 저장되어 있으며 이 값은 매 인증마다 변하게 된다. 따라서 사용자에 대한 개인 식별 정보는 저장되지 않는다.

(3) 무작위 대입 공격

Philips 시스템에서는 H(PK||RAN) 값과 RAN 값이 노출되었을 경우, 오프라인 상에서 무작위 대입을 통하여 PK에 대한 유추가 가능하다. 한편, PADRM 시스템에서는 최초 라이센스 발급 단계에서 노출될수 있는 값은 OTP와 TID이다. 따라서, PK와 SEED를 동시에 유추하여야 한다. 이러한 경우, Philips 시스템에서 PK에 대한 무작위 대입 공격에 걸리는 시간이 E(P)일 경우로 가정해 보면, PADRM 시스템에서는 PK에 대한 무작위 대입 공격 시간이 $E(P)^2$으로 상대적으로 안전한 편이다.

〈표 3〉 안정성 분석 결과 요약

	Sniffing 공격	Replay 공격	서버 침해 공격	무작위 대입 공격
HKUST	×	×	×	×
Philips	×	×	△	×
PADRM	○	○	○	△

* × : 안전하지 않음
* △ : 상대적으로 안전함
* ○ : 안전함

안전성 분석에 대한 결과를 요약한 내용이 〈표 3〉에 나타나 있다.

HKUST의 시스템에서는 보안 문제에 관해서는 특별히 언급하지 않고 있다. 따라서 개인 정보에 대한 안전을 보장할 수 없다. 한편, Philips 시스템은 가로채기 및 재연 공격에 취약함을 보이며, 서버 침해 공격에서 개인 식별 정보가 노출될 위험이 있다. 무작위 대입 공격은 PADRM시스템이 Philips 시스템보다 상대적으로 안전함을 보이고 있다.

5. 결 론

인터넷의 발전은 디지털 콘텐츠의 유통이라는 새로운 패러다임을 가져왔다. 디지털화된 자료는 보관과 전달이 용이하며 정보의 전달이 손쉬우므로 편리하나, 정보 융합 및 복제의 용이성과 함께 광범위하고 신속한 전달성, 통제의 곤란성이 존재하고 있다. 따라서 디지털 콘텐츠의 유통에는 DRM시스템이 필수적이다.

그러나 현재의 DRM 시스템은 사용자의 프라이버시 보호에 한계가 있다. DRM에서의 프라이버시를 향상하기 위한 여러 기술적 방법들이 제안되었으나, 대부분의 방법들은 현실적 적용에 있어서 많은 문제점을 가지고 있다.[6][7][9] 또한 향후 보급될 차세대 기술인 웹서비스 환경에 적합하지 않아 유비쿼터스 시대로 들어서게 되면 서비스 제공에 많은 어려움이 존재할 것이다. 이에 따라 HKUST의 Sai Ho Kwok은 워터마크 기술을 기반으로 한 웹서비스 DRM 시스템을 제안하여 워터마킹 기법을 구체적으로 웹서비스에 적용하였다.[2] 그러나 HKUST가 제안한 방법은 사용자에 대한 프라이버시 고려를 하지 않고 있어 실제 웹서비스 적용에 어려움이 있다. 또한 유비쿼터스 환경을 고려하지 않아 상황(Context)변화에 적응적(Adaptive)으로 서비스를 제공할 수 없다. 따라서 사용자의 Context를 고려한 서비스 제공은 불가능하다.

한편, 네덜란드의 필립스 연구소에서는 신원 기반의 DRM 시스템에 대한 문제점을 지적하고 이에 대한 프라이버시 대책을 제안하였다.[1] 그러나 해당 연구에서는 사용자와 기기간 전달되는 인증 정보가 노출될 경우 Sniffing/Replay 공격이 가능하여 부정한 사용자의 접근이 가능하다. 또한 콘텐츠의 이용자와 콘텐츠 재생 장치, 콘텐츠 제공자의 3가지의 영역에서 사용자의 PK에 대한 보호 중심으로 제안하고 있어 웹서비스와 같은 환경에 실제로 적용하는데 제약이 있다.

본 연구에서는 이러한 단점을 보완하여 유비쿼터스 웹서비스 환경에서 프라이버시를 보호할 수 있는 Privacy-Aware DRM 아키텍처를 제안하였다. 제안한 아키텍처는 익명성을 보장한 상태에서 콘텐츠에 대한 라이센스를 취득할 수 있다. 웹서비스는 근본적으로 SOAP 메시지의 교환을 통하여 서비스가 제공된다. 본 논문에서는 OTP 메커니즘을 기반으로 사용자에 대한 익명성과 함께 Sniffing/Replay Attack에 안전하게 라이센스 정보를 획득하고 SOAP 메시지상에 라이센스와 Context 정보를 포함하여 콘텐츠 제공자가 적응적(Adaptive)이고 적시적(Just-in-Time)인 서비스를 제공할 수 있는 구조를 제

안하였다.

DRM 기술과 개인정보보호는 항상 쟁점에 서 있다. 본 논문에서 제안한 방법으로 프라이버시를 보호하면서 디지털 저작권에 대한 관리가 가능하다. 또한, 향후 진행될 유비쿼터스 시대에 적합하고 사용자의 상황에 맞게 가공된 콘텐츠를 제공할 수 있다.

향후 과제는 PADRM에 구체적으로 Privacy Ontology를 고려하고 이러한 내용에 따라 실제 PADRM 시스템을 구현해 보고자 한다.

참 고 문 헌

[1] Claudine Conrado, Frank Kamperman, Geert Jan Schrijen, Willem Jonker, "Privacy in an Identity-based DRM System", Philips Research, 2002

[2] SAI HO KWOK, SIU MAN LUI, S. C. CHEUNG, AND KAR YAN TAM, "Digital Rights Management in Web Services", Hong Kong University Science Tehnology(HKUST), 2002

[3] 박남제, 송유진, "디지털 콘텐츠 저작권 보호기술", 정보보호학회 학회지 11권 5호, 2001. 10

[4] 고려대학교, "개인정보보호를 위한 기술 개발 및 기술정책", 한국전산원, 2004. 9

[5] 전종홍, 이원석, 이강찬, 김홍기 "시맨틱 웹서비스 기술동향 : DAML-S", 주간기술동향, 2003

[6] 이남용, "디지털 저작권과 프라이버시의 경합과 균형", 정보보호학회 14권 6호, 2004.12

[7] Ann Cavoukian, "Privacy and Digital Rights Management (DRM): An Oxymoron?", Information and Privacy Commissioner/Ontario, 2002

[8] MSDN, "WS-Security Profile for XML-based Tokens", Microsoft, 2002

[9] Joan Ferienbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, "Privacy Engineering for Digital Rights Management Systems", Yale Universty Science Dept, 2001

[10] Larry Korba, Steve Kenny, "Towards Meeting the Privacy Challenge : Adapting DRM", National Research Council of Canada, 2001

[11] Heng Guo, "Digital Rights Managment Using XrML", Helsinki Universty of Technology, 2001

[12] Arif Tumer, Asuman Dogac, I. Hakki Toroslu, "A Semantic based Privacy Framework for Web Services",Middle East Technical University, 2003

[13] Markus Keidl, Alfons Kemper, "Towards Context-Aware Adaptable Web Services", ACM, 2004

[14] Olli Pitkanen, Mikko Valimaki, "Towards A Digital Rights Management Framework", Helsinki Institute for Information Technology

저 자 소 개

송유진 (E-mail : song@dongguk.ac.kr)

1982. 한국항공대학교 졸업(학사)

1987. 경북대학교 대학원 졸업(석사)

1995. 일본 Tokyo Institute of Technology 졸업(박사)

1988. ~ 1996. 한국전자통신연구원 선임연구원

2003.12 ~ 2005.2 미국 University of North Carolina at Charlotte 연구교수

1996. ~ 현재 동국대학교 전자상거래학과/대학원 교수

2005. ~ 현재 동국대학교 부설 전자상거래연구소 소장

1998. ~ 현재 한국정보보호학회 이사

1997. ~ 현재 한국정보시스템학회 이사

2001. ICISC2001 운영위원장 역임

2003. 하계CISC2003 프로그램 위원장

관심 분야 전자상거래응용 보안 (Ubiquitous/Web Service Privacy, Location Privacy, 디지털콘텐츠 보호, XML보안, SCM/CRM 보안 등), Context Aware Application Security

이동혁 (E-mail : jazzbop@korea.com)

2004. 동국대학교 전자상거래학과 (학사)

2005. ~ 현재 동국대학교 전자상거래학과 석사과정

관심 분야 XML 보안, 유비쿼터스/웹서비스 프라이버시 보호, 전자상거래 보안