디지털 자료의 배포와 이용을 효과적으로 제어하기 위한 Access Control에 관한 연구

김대엽*, 주학수**, 임종인***

*삼성종합기술원, **한국정보보호진흥원, ***고려대학교 정보보호대학원

A Study on Access Control for Controlled Digital Content Dissemination and Usage

Dae-Youb Kim*, Hak-Soo Ju**, Jong-In Lim***

*SAIT, **KISA, ***Korea Univ.

요 약

인터넷 인프라의 보급과 이용인구의 급속한 증가는 off-line을 통해서 물리적으로 획득하던 다양한 정보와 자료를 인터넷을 통해서 쉽고 빠르게 이용할 수 있는 서비스를 창출하고 있다. 그러나 이와 같은 서비스를 통해서 제공되는 컨텐츠의 저작권 문제와 불법 복제 등과 같은 피해도 함께 증가하고 있다. 이런 문제를 해결하기 위해서는 컨텐츠에 접근하고 이용할 수 있는 자격을 가지고 있는 사용자만이 해당 컨텐츠를 정상적으로 이용할 수 있도록 하는 Access Control(AC) 기술이 함께 연구되고 있다. 현재 상용화되어 있는 CAS와 DRM은 PBT 형태의 대표적인 AC 기술이라 할 수 있다. 본 논문에서는 [5]에서 제시된 PFT 기반의 AC를 위한 Security Architecture를 살펴보고, 효과적인 운영을 위한 PFT 기반의 새로운 AC 구조를 제시한다.

Ⅰ. 서론

인터넷 이용인구의 급속한 증가와 인프라의 보급, 그리고 위성, 케이블 등을 이용한 다양한 전송 매체의 발달은 기존의 off-line을 통해서 물리적으로 이용하던 다양한 정보와 자료들을 사용자들이 on-line을 통해서 쉽게 이용하도록 제공하는 서비스를 창출하게 되었다. 또한 이와 같은 서비스들은 각종 mobile 단말기와 wireless internet이 보급되면서 서비스의 종류와 이용자의 수가 급속히 증가될 것으로 예상된다. 그러나 이러한 서비스를 지속적으로 제공하고, 컨텐츠의 질을 높이기 위해서는 사용자의 인증 및 개인 정보 보호 뿐 아니라 저작권자의 권리 보호와 유료서비스를 통한 효과적인 사용료 징수 등의 문제가 함께 해결되어야 한다.

Access Control(AC)은 저작권 보호와 컨텐츠의 유료 서비스를 제공하기 위하여 사용되는 방법 중 하나 이다. Access Control 기술을 사용해서 유료 컨텐츠 서비스를 제공하는 대표적인 시스템으로 제한 수신 시스템(Conditional Access System, CAS)과 디지털 저작권 관리 시스템(Digital Right Management System, DRM)을 들 수 있다. CAS는 디지털 위성 및 케이블을 통해서 전송되는 A/V 및 데이터를 스크램블(Scramble)된 상태로 제공하고, 해당 프로그램에 대한 이용 권한을 소유한 수신자만이 디스크램블(Descramble)을 통해서 서비스를 이용할 수 있도록 필요한 정보를 제공해 주는 시스템을 의미한다. 이와 같은 서비스를 제공하기 위해서 CAS에서는 스크램블러와 디스크램블러, 그리고 가입자 스마트카드와 같은 장비가 필요하며, 효과적인 가입자 자격 제어를 위하여 일반적으로 ECM(Entitlement Control Message)과 EMM(Entitlement Management Message)을 사용한다[1][2][3].

DRM은 저작권 보호를 위해 허락 받은 사용자(라이선스를 받은 사용자)만이 허용된 규칙에 따라 컨텐츠를 사용하도록 지원하고, 불법적인 접근과 사용을 방지하는 시스템이다. 즉, 적법하게 라이선스(license)를 발급 받은 자만이 라이선스가 허용하는 사용규칙에 따라 해당 컨텐츠를 이용할 수 있도록 제어한다. 이와 같은 서비스를 제공하기 위하여 DRM에서는 사용자에게 제공되는 응용 프로그램(Virtural Machine, VM)과 라이선스를 이용한다. 제공되는 컨텐츠와 라이선스는 암호화된 상태로 제공되며, 사용자 VM을 통하여 복호화와 확인 과정을 거쳐서 이용하게 된다[4][5][6].

CAS와 DRM이 프로그램이나 컨텐츠의 사용료

를 효과적으로 징수할 수 있도록 설계된 Payment-Base Type(PBT)의 Access Control 구조를 갖는다면, PBT와 다른 또 하나의 구조로 Payment-Free Type(PFT)의 Access Control을 고려해 볼 수 있다. PBT에서 디지털 컨텐츠의 배포 및 사용은 해당 컨텐츠의 접근 및 사용에 따른 요금 정책을 기본으로 전체 시스템을 제어한다. 즉, 모든 디지털 컨텐츠에는 대응되는 사용료와 관련된 정보가 할당되고, 이 정보에 따라서 정당한 값을 지불하고 해당 컨텐츠에 대한 접근 및 사용 권리를 소유한 사람만이 컨텐츠를 이용할 수 있다. PFT는 컨텐츠의 접근 및 사용을 제어하기 위하여 사용료 지불 정책을 기본으로 사용하지 않고, 시스템 구성 요소들의 신뢰성과 보안과 관련된 요소에 의하여 전체 시스템을 제어한다. 그러나 Payment Gateway나 다른 지불과 관련된 기능을 첨가하여 상업적인 서비스에 충분히 이용할 수 있다. 이와 같은 PFT 서비스는 실생활에서 쉽게 찾을 수 있다. 예를 들어 정부문서 보관소에 저장되어 있는 문서에 대한 접근 통제나, 기관 사이에 교환되는 문서의 접근 통제 등이 있을 수 있다.

이와 같은 AC 구조의 설계에 있어서 반드시 고려되어야 하는 것은 안전성과 효율성 뿐 아니라 사용자 편리성이다. 본 논문에서는 먼저 [7]에서 제시된 PFT 관점에서 Security Architecture를 살펴보고, 그 특징을 간략하게 기술한다. 또한 효율성과 편리성을 증가시킬 수 있는 새로운 구조를 제시한다. 본 논문의 목적은 새로운 AC 구조의 제안에 둔다. 그러므로 제시된 구조의 구체적인 안전성 문제는 시스템 설계 및 구현에 관한 문제이기 때문에, 본 논문의 범위를 벗어나므로 여기서는 다루지 않고, 대략적인 필요성만 실명한다.

Ⅱ. 본론

1. Security Architecture

이 절에서는 [7]에서 제시된 Security Architecture에 관하여 살펴보고, 그 특징을 알아본다.

1) 구성 요소

Security Architecture를 구분하는 세 가지 요소는 다음과 같다:

- 응용프로그램 (Virtual Machine, VM)
- 사용 규칙 (Control Set, CS)
- 컨텐츠 배포 형식 (Distribution Style).

VM은 사용자의 컴퓨터에서 사용되는 S/W로 컨텐츠에 대한 사용자의 이용을 제어하기 위한 기능이 탑재되어 있다. 일반적으로 디지털 컨텐츠는 접근 제어를 위하여 암호화나 다른 보안기술을 이용해서 encapsulation된 상태로 사용자에게 제공되며, 이렇게 제공된 컨텐츠는 Distributor(배포자) 또는 Control Center가 제공한 특정 VM을 통해서만 접근할 수 있다. CS는 접근 권한이나 사용규칙을 명시한 목록으로 사용자의 컨텐츠 접근과 이용을 제어하기 위하여 VM에서 사용된다. CS는 크게 Fixed Control Set, Embedded Control Set, External Control Set으로 구분된다. 배포 형식은 Message Push(MP)와 External Repository(ER)로 구분된다. MP에서 디지털 컨텐츠는 각각의 사용자에게 직접 전송된다. ER에서는 네트워 상에 있는 컨텐츠 배포 서버(Repository Server, RS)를 통해서 사용자가 컨텐츠를 이용할 수 있다.

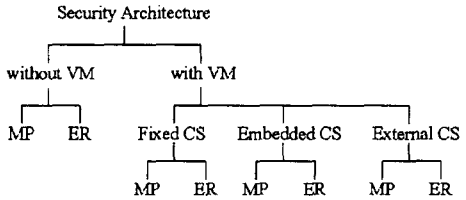

그림 1 : Security Architectures.

2) Security Architectures와 특징

그림1은 [7]에서 제시된 Security Architecture를 요약한 것이다. 제시된 구조는 사용자 측면에서 VM의 필요여부에 따라 두 가지 종류로 구분되며, VM을 사용하는 경우는 다시 CS의 형태에 따라 세 종류로 구분된다. 또한, 모든 형태의 AC는 컨텐츠 배포 형식에 따라 각각 MP와 ER로 세분화된다.

컨텐츠는 접근 제어를 위하여 encapsulation 된 상태로 배포되는데, 이와 같이 encapsulation 시킨 결과를 Digital Container(DC)라고 부른다. w/oVM의 경우는 DC를 열 수 있는 도구가 사용자에게 없기 때문에 encapsulation 되지 않은 컨텐츠가 배포된다. 이 경우, 컨텐츠가 배포된 이후에 해당 컨텐츠에 대한 접근 및 사용을 직접적으로 제어할 수 있는 방법이 없다. 그러므로, 해당 컨텐츠에 대한 불법적인 배포 및 도난 등이 증가할 수 있다.

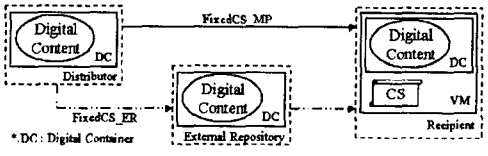

그림 2 : Fixed CS 형태의 AC

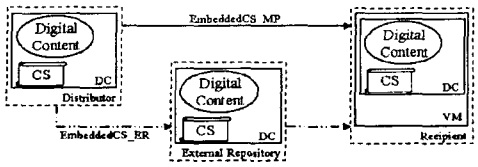

그림 3 : Embedded CS 형태의 AC.

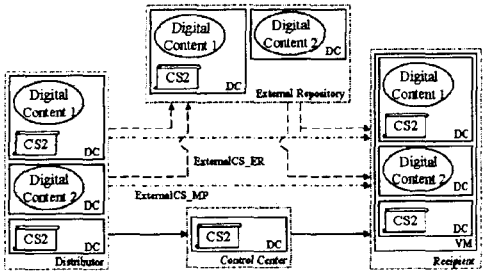

그림 4 : External CS 형태의 AC.

그림 2는 Fixed CS 형태의 AC 시스템의 운영을 설명하고 있다. Fixed CS는 컨텐츠의 접근과 사용을 제어하기 위해 필요한 CS가 VM에 고정된 상태로 VM이 배포될 때 함께 사용자에게 전달된다. 그러므로 디지털 컨텐츠에 대응되는 특정 VM이 없이는 해당 컨텐츠를 이용할 수 없으며, 접근 제어는 기본적으로 VM에 내장된 CS를 따라서 이루어진다. CS가 VM에 고정된 상태로 내장되어 배포되기 때문에, 배포가 완료된 이후에 CS를 변경하는 것이 어렵다. Fixed CS의 경우, 컨텐츠의 재분배는 해당 컨텐츠를 이용할 수 있는 CS가 내장된 VM을 소유한 사용자들 사이에서만 가능하다.

Embedded CS 형태의 AC 시스템은 그림 3에서 볼 수 있듯이 디지털 컨텐츠를 배포하기 위해 사용하는 DC에 컨텐츠와 함께 CS를 encapsulation 시켜서 전송한다. 배포된 디지털 컨텐츠에 대한 접근 및 이용 제어는 DC에 포함된 CS를 통해서 이루어진다. 일반적으로 CS를 관리하는 Control Center가 없기 때문에 보급자는 배포된 컨텐츠에 대한 CS를 변경할 수 없다.

그림 4에서처럼, External CS 형태의 AC 시스템은 디지털 컨텐츠와 해당 컨텐츠를 이용하기 위해 필요한 CS를 독립적으로 운영하는 형태를 갖는다. encapsulation 된 컨텐츠는 배포 방식에 따라 배포자가 직접 사용자에게 배포하거나 또는 배포자가 RS에 컨텐츠를 저장하면, 사용자가 필요한 컨텐츠를 RS에 접속해서 획득한다.

External CS 형태의 AC에서 사용자의 컨텐츠 사용 권한을 나타내는 CS를 운영하는 방법은 다음과 같은 두 가지 종류가 있다. 첫째는 컨텐츠를 획득한 사용자(또는 사용자의 VM)는 해당 컨텐츠사용에 필요한 CS를 Control Center에 요청하고, 이를 발급 받아 사용한다. 둘째는 컨텐츠(예, digital content 1)를 전달할 때 다른 컨텐츠(예, digital content 2) 이용에 필요한 CS(예, CS2)를 함께 전달하는 것이다. 그러나 후자의 경우 실제 운영에 있어서 Digital Content 2를 사용하기 위해 필요한 CS2가 Digital Content 1과 함께 encapsulation 되어 있음을 알려주는 추가적인 정보가 필요하다는 단점 때문에 전자의 방법이 보편적으로 이용되고 있다. External CS 형태를 갖는 AC는 컨텐츠와 CS를 독립적으로 운영하므로 CS의 변경과 갱신이 용이하다. 단, Control Center는 컨텐츠 배포자와 이용자가 모두 신뢰할 수 있는 기관으로 실제 서비스에서는 CS의 관리뿐 아니라 사용자의 컨텐츠 사용 이력도 함께 관리한다.

2. 컨텐츠 Access Control 제안

Fixed CS의 경우 VM이 배포된 이후에 내장된 CS를 변경하는 것이 어렵다. Embedded CS의 경우, 모든 사용자에게 동일한 CS를 적용하지 않는다면, 사용자의 요구에 따라 DC를 새로 만들어야 한다. 이는 사용자와 컨텐츠의 수가 증가할 수록 DC를 생성해야 되는 컨텐츠 배포자에게 많은 작업을 요구하게 된다. External CS의 사용자는 디지털 컨텐츠와 대응되는 CS를 함께 획득해야 해당 컨텐츠를 이용할 수 있고, 필요에 따라서는 사용자 요구에 따라 새로운 CS와 DC를 만들어야 된다.

이와 같은 문제는 근본적으로 사용자와 VM을 대응시켜 사용하거나, 컨텐츠와 CS를 일대일 대응시켜서 사용하기 때문에 발생한다. 또한 이러한 구조에서는 서비스 제공자(SP)나 컨텐츠 제공자(CP)가 자신들이 소유한 정보, 프로그램, 그리고 컨텐츠 등에 대하여 현재 위성방송에서 제공하는 것과 같은 다양한 서비스를 사용자에게 제공하기 힘들다. 뿐만 아니라 off-line 전용 또는 범용 장치를 사용해서 해당 컨텐츠를 이용하려는 사용자에게는 서비스를 제공할 수 없다.

이처럼 기존의 AC 구조들이 갖고 있는 문제점을 해결하고, 컨텐츠 운영자(여기서는 Control Center)에 의한 다양한 서비스가 가능하도록 하기 위하여 두 종류의 CS, recipient_CS(r_CS)와 originate_CS(o_CS)를 이용한 External CS 형태의 새로운 AC 구조를 제안한다.

1) Control Set

제안하는 AC 구조에서는 컨텐츠 사용에 대하여 해당 컨텐츠 소유권자의 요구사항을 명시한 o_CS와 서비스 제공자로부터 컨텐츠를 공급받아 이용하려는 사용자의 권한을 나타내는 r_CS를 통해서 컨텐츠의 배포 및 이용을 제어한다. 제안하는 구조에서 Control Center는 서비스 사업자 또는 서비스 운영자의 역할을 병행한다고 가정한다. 본 논문에서 서비스는 사용자로 하여금 다양한 방법으로 컨텐츠를 이용할 수 있도록 제공하는

것을 의미한다. 즉, 컨텐츠를 하나씩 이용하는 개별 서비스 뿐 아니라, 컨텐츠 패키지 서비스, 컨텐츠 예약 서비스 등을 예로 들 수 있다.

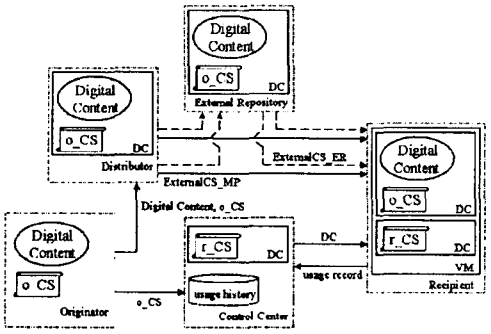

그림 5 : 두 개의 CS로 운영되는 새로운 AC.

o_CS는 컨텐츠의 소유권자(또는, 저작권자)에 의해서 생성되며, 해당 컨텐츠를 이용하기 위해서 사용자가 충족시켜야 되는 조건들을 나열한 목록을 포함한다. 사용자가 컨텐츠를 이용하기 위해서는 o_CS에 명시된 조건들을 전부 또는 일부 만족시켜야 된다. 생성된 o_CS는 Control Center에 제출되고, 해당 컨텐츠와 함께 배포자에게 전달된다. 배포자는 컨텐츠와 o_CS를 함께 encapsulation 시켜서 DC를 생성한다.

o_CS는 기본적으로 Control Center로부터 할당받은 컨텐츠 고유 id와 서비스 사업자에 의해서 분류된 해당 컨텐츠의 종류 및 성격을 포함한다. 또한, 컨텐츠 사용에 따른 소유권자의 요구 사항 목록을 포함한다. 예를 들어 해당 컨텐츠를 사용할 수 있는 지역, 사용자 연령 뿐 아니라 사용자 등급에 따른 컨텐츠 기본 이용 권한(읽기, 인쇄, 편집 등)과 이용 횟수 제한 등이 요구 사항이 될 수 있다. 또한 특정 사용자만 사용하도록 사용자 id를 명시할 수도 있다.

컨텐츠 id를 근거로 r_CS(사용자의 컨텐츠 사용 권한으로 뒤에서 자세히 설명한다.)에 동일한 컨텐츠 id가 포함되어 있을 때만, 사용자가 해당 컨텐츠를 이용할 수 있도록 제한하면, [7]에서 제시된 External CS 형태의 AC와 동일한 서비스를 제공할 수 있다. 뿐만 아니라, o_CS와 r_CS에 명시된 컨텐츠 id와는 상관없이 컨텐츠 이용에 필요한 사용자 조건만 검증되면 누구나 해당 컨텐츠를 이용할 수 있도록 설정할 수 있다.

Payment Gateway등과 같은 지불 시스템과 함께 시스템을 구성한다면 o_CS는 해당 컨텐츠 이용에 따른 요금 정보를 포함할 수 있다. 또한, 컨텐츠의 종류나 컨텐츠 id와 관계없이 사용자의 컨텐츠 접근 및 해당 컨텐츠의 사용에 따라 요금을 징수하는 서비스(Pay-Per-Usage, PPU) 제공 여부와 PPU 서비스에 따른 요금 정보를 함께 기록함으로써 특정 컨텐츠와 관련된 CS 없이도 사용자가 원하는 컨텐츠를 (공급받는 방법에 상관없이) 이용할 수 있다.

r_CS는 서비스 사업자가 제공하는 컨텐츠 서비스를 제공받기 위하여 사용자가 Control Center에 신청해서 발급 받는다. 기존의 AC 구조에서 CS가 컨텐츠를 이용하기 위해 발급 받는 것이었다면, 제안하는 구조에서는 컨텐츠 서비스를 이용하기 위하여 발급 받는다는 차이가 있다.

r_CS는 기본적으로 사용자 인증정보와 컨텐츠 사용 권한 목록으로 구성된다. 사용자 인증정보에는 Control Center가 부여한 사용자 id를 비롯해서 사용자의 연령, 지역, 직업 및 서비스 이용 등급 등 사용자 인증에 필요한 정보가 모두 포함된다. 컨텐츠 사용 권한 목록에는 서비스 사업자가 제공하는 서비스 목록 중에서 사용자가 선택한 서비스와 해당 서비스 또는 서비스에 포함된 컨텐츠의 사용 권한(예를 들어, 1회 복사, 출력, 편집 등)으로 구성된다. 지불 시스템과 함께 운영된다면, 유료 컨텐츠 사용에 필요한 토큰(Token)과 PPU 서비스 이용 가능 여부 등이 명시될 수 있다. 사용자 인증 정보는 사용자가 해당 서비스 사업자에게 등록할 때 한번 생성된 정보를 계속 이용할 수 있으나, 사용 권한 목록은 사용자가 서비스를 신청 또는 변경할 때마다 새로 생성해야된다.

2) 운영

앞서 언급했던 것처럼 제안하는 AC 구조를 효과적으로 운영하기 위해서, Control Center는 기존의 CS 관리와 Usage History 관리 이외에 사용자와 컨텐츠 소유권자 사이에서 다양한 서비스 제공할 수 있어야 한다. 또한 r_CS의 발급을 위해서 PKI의 RA/CA와 같이 사용자를 확인하고 검증하는 기능도 수행해야한다. 그리고 지불 시스템과 연동된 경우, 관련 정보의 관리 및 운영에 관한 모든 책임도 갖는다.

제안하는 AC의 운영 순서는 다음과 같다:

① 컨텐츠 등록 : 컨텐츠 소유권자는 Control Center에 해당 컨텐츠를 등록하고, 컨텐츠 id와 컨텐츠 분류 정보(예를 들어 종류, 성격, 시청 연령 등)를 할당받아 o_CS를 작성하고, Control Center에 제출한다. 컨텐츠와 o_CS를 배포자에게 전달해서 encapsulation 과정을 거쳐 DC로 생성/배포한다.

Control Conter는 제출된 o_CS와 기존의 다른 컨텐츠의 o_CS를 가지고 소유권자와의 계약에 따라 서비스를 구성해서 사용자에게 제시한다.

② 사용 권한 신청 : 컨텐츠 사용자는 Control Center에 등록하고, 사용자 id 및 인증정보를 부여받는다. Control Center에서 제시한 서비스 목록을 검토하고, 원하는 서비스와 해당 서비스에 포함되어 있는 컨텐츠의 사용 자격을 신청한다. 유료 서비스가 제공되는 경우, 해당 서비스 이용을 위한 Token을 신청한다. 또한 PPU 서비스가

제공되는 경우, PPU 서비스 이용허가를 신청한다.

Control Center는 사용자 요청에 따라 r_CS를 적절하게 구성하고, 사용자에게 전송한다. 사용자는 전송받은 r_CS를 VM에 입력한다.

③ 컨텐츠 획득 : 컨텐츠 사용자는 컨텐츠 배포자나 RS로부터 컨텐츠 DC를 전송 받아 사용자 VM에 입력한다.

④ 컨텐츠 사용 : VM은 입력된 r_CS와 o_CS의 입력을 확인한다. 입력된 r_CS와 o_CS를 근거로 해서 r_CS 소유자를 인증하고, 소유자가 해당 컨텐츠에 접근할 수 있는지를 판단한다. 이 때, r_CS의 사용자 인증정보가 o_CS에 명시된 연령, 등급 등 컨텐츠 접근에 필요한 모든 조건이 동시에 만족 할 때만 접근을 허가한다.

그리고 해당 컨텐츠의 사용 권한을 확인해서 컨텐츠 사용을 제어한다. 예를 들어, 전자문서의 o_CS에 3급 이상의 서울지역 공무원만 읽을 수 있도록 설정되어 있다면, r_CS에 포함된 사용자 인증 정보에서 "3급 이상, 서울, 공무원" 이라는 조건이 만족되어야 하고 컨텐츠 사용 권한 목록 중에서 읽기가 설정되어 있어야만 한다.

만약 지불 시스템과 연동 중이고, 해당 컨텐츠가 (후불 서비스에서) 유료라면 이용료 지불에 충분한 Token이 있어야 한다.

⑤ PPU 서비스 : 지불 시스템과 함께 운영 중이고 해당 컨텐츠에 대하여 PPU 서비스가 제공되고 있는 경우에 VM이 o_CS와 r_CS를 확인한 결과, 사용자가 해당 컨텐츠에 대한 접근 권한을 갖고 있지 않다고 판단되면, PPU 서비스를 받을 것인지를 사용자에게 확인을 받아 해당 서비스를 제공할 수 있다. PPU 서비스를 제공하기 위해서는 사용자가 PPU 서비스로 이용한 컨텐츠 목록을 Control Center가 (이용과 동시에 또는 이용 후에) 수집할 수 있어야한다. 이렇게 수집된 이용 정보는 사용자에게 해당 컨텐츠 이용에 따른 사용료 징수와 저작권료 지불을 위한 근거 자료로 사용될 수 있다.

3) 특징 및 문제점

기존의 CS가 '컨텐츠'에 대한 사용 자격을 제어하기 위해서 사용되었다면, 제안된 AC 구조에서는 '컨텐츠 서비스'에 대한 사용 자격으로 그 범위를 확장시킴으로 다양한 서비스를 제공할 수 있다. 특히 기존의 구조에서는 사용될 수 없었던 PPU나 사용자의 특정 조건만을 확인해서 컨텐츠를 이용하게 하는 서비스가 가능하다.

컨텐츠를 사용하기 위해 Control Center에 접속할 필요가 없기 때문에 컨텐츠를 이용할 때마다 Control Center에 접속해야 되는 기존의 구조에 비하여 접속횟수를 상당히 줄일 수 있다. 또한 기존의 구조에서는 네트워크에 연결된 PC등에서만 사용 가능했지만, 제안하는 구조는 VM이 장착된 모든 장치(예를 들어 CDP, MP3 Player, PDA 등)에 r_CS를 입력시키는 것만으로 이용이 가능하다.

그러나 이와 같은 서비스를 실제 구현하기 위해서는 r_CS를 안전하게 운영하는 방안과 유료 서비스를 위한 지불 시스템과의 연동 등이 해결되어야 한다. 특히, r_CS의 분실 및 불법 복제와 같은 문제를 해결해야 되며, 사용자 인증 문제 또한 풀어야 될 과제다. 이와 같은 문제는 VM과 r_CS를 대응시켜서 운영하는 방안과 스마트카드와 같은 안전한 저장 매체를 이용하는 방안 등을 고려해 볼 수 있다. r_CS를 저장하고 있는 DC나 r_CS 안에 사용자 비밀번호를 hash된 상태로 저장시켜 놓고, VM에서 사용자의 비밀 번호를 확인하는 방안도 부가적으로 고려해 볼 수 있다. 앞서 언급한 것처럼 본 논문의 목적이 새로운 AC 구성을 제안하는 것이므로 안전성에 관한 자세한 언급은 생략하도록 한다.

Ⅲ. 결론

본 논문에서 제안한 AC 구조는 기존에 제안된 구조가 컨텐츠를 이용할 때마다 CS를 획득해야하거나, VM을 공통적으로 이용할 수 없다는 단점을 감안해서 컨텐츠 소유권자가 작성한 o_CS와 컨텐츠 사용자의 요청에 따라 Control Centerd가 생성한 r_CS를 통해서 사용자가 필요에 따라 미리 원하는 컨텐츠들의 사용 권한을 확보해 둘 수 있도록 설계되었으며, PPU와 같은 서비스가 가능하도록 구성하였다. 이를 위하여 컨텐츠 기반의 제어가 아닌 컨텐츠 서비스 기반의 제어를 선택했다. 특히, 제안한 AC 구조에서 VM은 o_CS와 r_CS를 검증하고, 그 결과에 따라 컨텐츠를 사용할 수 있도록 제공하는 역할만을 수행하기 때문에 특정 사용자나 컨텐츠에 관계없이 사용될 수 있다. 그러므로, r_CS를 스마트카드와 같은 안전한 저장 장치와 함께 운영한다면 쉽게 사용자 플랫폼을 변경해서 사용할 수 있으며, 사용자 플랫폼이 CDP와 같은 오프라인 장치라도 응용이 가능하다. 또한 제안된 AC 구조는 DRM과 같은 컨텐츠 유료 서비스 뿐 아니라 디지털 문서 보관소와 같은 PFT 서비스에도 적용이 가능하다.

앞서 언급한 것처럼 본 논문의 목적에 따라 제안된 구조는 운영의 안전성 측면을 충분히 고려하지 않았다. 그러므로 실제 시스템 설계 및 운영에 있어서 안전성 측면을 충분히 고려해야 되고, 서비스의 대중성을 위해서는 다양한 서비스 종류의 개발과 이를 지원할 수 있는 효과적인 Control Set의 설계가 계속 연구되어야 한다.

참고문헌

[1] EBU Project Group B/CA, "Functional model of conditional access system", EBU

Technical Review, pp.64-77, winter 1995.

[2] Francoise Coutrot, vincent Michon, "ASingle Conditional Access System for Satellite-Cable and Terrestrial TV", IEEE Trans. on Consumer Electronic, vol. 35, no. 3, pp 464-468, Aug. 1989.

[3] Didier Angebaud, Jean-Luc Giachetti, "Conditional Access Mechanisms for All-Digital Broadcast Signals", IEEE Trans. on Consumer Electronic, vol. 38, no. 3, pp 188-194, Aug. 1992.

[4] 이창열, "DRM 기술", 정보보호학회지 제12권,제1호, pp. 1-10, 2002년 2월.

[5] 전종민, 최영철, 박상준, 박성준, "DRM 기술 및 제품 동향 분석", 정보보호학회지 제 11권, 제5호, pp 26-34. 2001년 10월.

[6] Renao iannella, "Digital Rights Management Architectures", D-Lib Magazine, Volume 7, Number 6, June 2001.

[7] Park, Jachong, Ravi Sandhu., and James Schifalacqus., "Security Architectures for Controlled Digital Information Dissemination", Proceedings of the 16th Annual Computer Security Application Conference, 2000.