홍 승 필 교수지도

석사학위 청구논문

N-Screen 환경 내 신뢰할 수 있는 콘텐츠 이용 방안 설계 및 구현

2013

성신여자대학교 대학원

컴퓨터학과

신 유 진

N-Screen 환경 내 신뢰할 수 있는 콘텐츠 이용 방안 설계 및 구현

홍 승 필 교수지도

이 논문을 석사학위논문으로 제출함

2012년 11월

성신여자대학교 대학원

컴퓨터학과

신 유 진

인 준 서

신유진의 석사학위 논문으로 인준함.

심사위원 홍 의 석 인

심사위원 변 혜 원 인

심사위원 홍 승 필 인

성신여자대학교 대학원

논문 개요

본 논문에서는 N-Screen 환경 내에서 다양한 멀티미디어 콘텐츠를 보다 안전하고 유연성 있게 활용할 수 있는 방안을 제안한다. N-Screen 환경이란 스마트폰으로 대표되는 스마트 디바이스들의 확산으로 새롭게 등장한 서비스 패러다임이다. 한 명의 사용자가 다양한 스마트 디바이스를 소유하게 되면서 자연스럽게 사용자가 소유한 콘텐츠들의 OSMU(One Source Multi Use)에 대한 사항이 이슈가 되고 있다. 그러나 디바이스 및 모바일 OS의 벤더들의 정책이 서로 상이함에 따라 일관되지 않은 제조사의 기기 및 OS를 이용하는 사용자들에게 있어서 OSMU는 어려운 실정이다. 또한 급격하게 구축된 스마트 디바이스 환경에 따라 무분별한 콘텐츠의 유포 및 이용이 확산됨에 따라 스마트 디바이스 환경 내에서 신뢰할 수 있는 콘텐츠의 이용에 대한 요구가 증가하게 되었다.

이와 같은 문제점을 해소하고자 본 논문에서는 N-Screen 환경 내 신뢰할 수 있는 콘텐츠 이용 방안을 설계 및 구현한다. 본 논문에서는 NTCPM (N-Screen Trusted Content Provide Model)의 설계를 통해 분산 되어 있는 디바이스 및 OS 환경에서도 동일한 서비스를 이용할 수 있는 방안과 신뢰할 수 있는 콘텐츠를 제공하기 위한 방안을 연구하였다.

본 논문에서 제시한 모델을 통해 스마트 디바이스를 이용함에 있어 환경적인 제약을 받지 않고도 콘텐츠를 유연하게 이용하는 동시에 콘텐츠에 대한 여러 가지 검증을 통해 사용자에게 신뢰할 수 있는 콘텐츠를 제공할 수 있는 효과를 기대할 수 있다.

목 차

<그림 목차>

<표 목차>

Ⅰ. 서 론

최근 경량화 및 고성능화, 그리고 이동성을 갖춘 모바일 기기에 모바일 전용 OS를 탑재한 획기적인 스마트 디바이스의 등장으로 인해 모바일 단말은 점점 진화와 발전을 거듭하고 있다. 스마트폰을 주축으로 한 태블릿 PC 및 스마트 TV, 그리고 MP3, PMP와 같이 모바일 OS를 채택한 다양한 지능화 기기들의 등장으로 인해 멀티미디어 콘텐츠의 사용량 또한 폭발적으로 증가하게 되었다.

또한 한 명의 사용자가 다양한 스마트 디바이스를 소유하게 됨으로서 자연스럽게 사용자가 소유한 모바일 기기(모니터)를 서로 연동하여 모바일 기기에서 이용 가능한 콘텐츠들을 공유하고자 하는 움직임 또한 발생하게 되었다. N-Screen은 이와 같은 움직임에서 파생된 개념이라고 할 수 있다. N-Screen은 말 그대로 n개의 스크린이라는 뜻으로, 스마트폰, 스마트 TV, 태블릿 PC는 물론 MP3, PMP, 내비게이션과 같은 화면을 가지고 있는 모바일 기기들의 스크린을 통해 하나의 콘텐츠를 자유자재로 이용할 수 있는 것을 말한다. 이와 같은 새로운 모바일 환경 패러다임의 등장으로 인해 새로운 서비스 및 콘텐츠들이 모바일 기기를 통해 제공되고 있다.

그러나 스마트 기기를 통한 각종 서비스 및 콘텐츠의 이용 현황이 점점 늘어가는 추세임에 반해 다양한 보안상의 취약점으로 인해 안전한 이용이 어려운 실정이다. 스마트폰, 태블릿 PC와 같은 기기가 내재하고 있는 취약점은 물론 스마트 기기에서 이용되는 서비스 및 콘텐츠가 가지고 있는 보안의 취약성으로 인해 스마트 기기에서 활용되는 사용자의 개인정보에 대한 위협이 크게 대두되고 있다. 특히 스마트 디바이스를 이용한 각종 결제 및 금융 관련 서비스의 이용량이 증가하면서 이와 같은 문제는 심화되고 있는 추세이다.

따라서 본 논문에서는 N-Screen 환경 내에서 다양한 콘텐츠를 이용할 때 신뢰할 수 있는 콘텐츠의 제공을 위하여 'N-Screen 환경 내 신뢰할 수 있는 콘

텐츠 이용 모델'을 설계하고 구현함으로써 그 가능성을 타진한다.

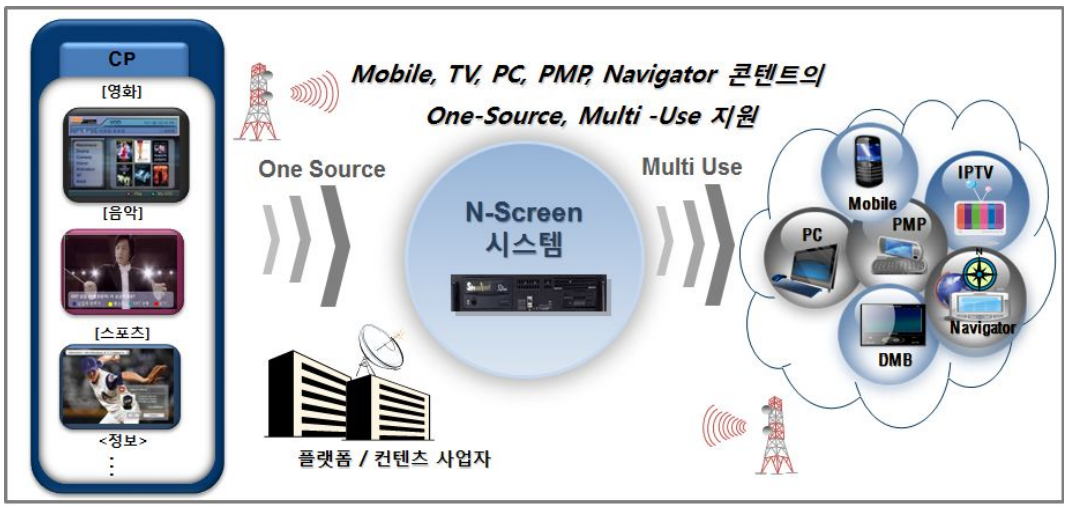
본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 N-Screen 및 개인정보 관련 기술 및, 법적 제도적 동향과 기존에 발표된 N-Screen관 관련된 모델에 대해 설명한다. 3장에서는 N-Screen 환경 내에서 콘텐츠를 이용할 시 야기될 수 있는 개인정보의 문제점을 언급하고, 4장에서는 NTCPM의 구조를 설계하고 기능을 설명한다. 5장에서는 NTCPM을 프로토타이핑하고 6장의 기대효과 및 향후 연구와 7장의 결론으로 구성된다.

Ⅱ. 관련 연구

1. N-Screen

1) 개요

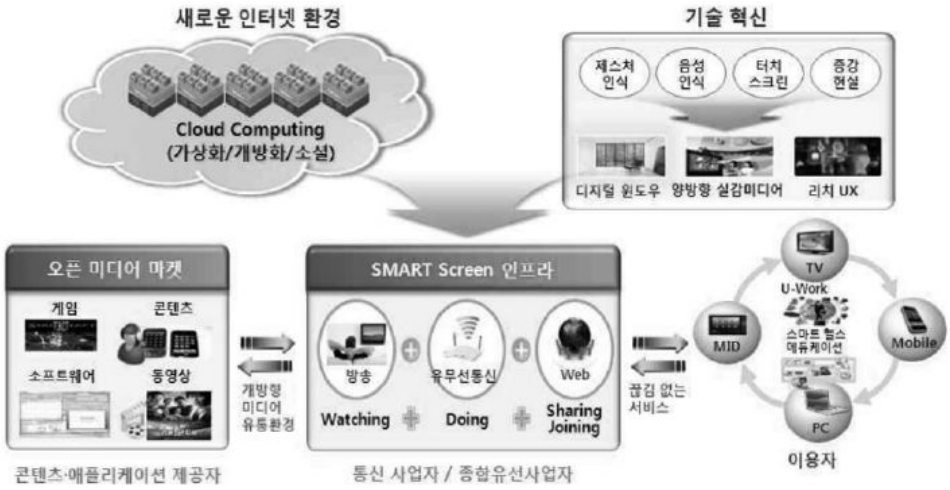
N-Screen이란 무선망과 인터넷의 초고속화와 함께 비디오 스트리밍, 모바일 방송, IPTV 등 방통융합 환경에서의 멀티미디어 콘텐츠가 보편화되고, 이종의 접속망과 다양한 성능의 단말이 혼재하는 융합 콘텐츠 환경에서 스마트폰, 태블릿 PC, MP3, PMP, 내비게이션 등의 다양한 단말에서 비디오, 음악, 게임, 텍스트 데이터와 같은 콘텐츠를 끊김 없이 이용할 수 있는 서비스를 일컫는다.[1] 다음 그림은 N-Screen의 개요도이다.



[그림 1] N-Screen 개요도

N-Screen은 최근 등장하게 된 스마트폰, 스마트 TV, 태블릿 PC와 같은 개인용 콘텐츠 플랫폼이라 할 수 있는 스마트 디바이스들의 성장 및 언제 어디서나 인터넷에 연결될 수 있도록 하는 무선 네트워크의 확산을 통해 자연스럽게 등

장한 개념이라고 할 수 있다. 한 사람의 사용자가 다양한 멀티 디바이스를 소유하게 됨으로서, 각각의 디바이스에서 다양한 멀티미디어 콘텐츠를 이용할 수 있게 되었고 이와 같은 패러다임의 변화는 시간과 장소에 관계없이 사용자가 콘텐츠를 향유할 수 있는 환경을 제공할 수 있게 되었다.



[그림 2] N-Screen 서비스의 예시

N-Screen 서비스는 미국의 최대 통신사업자인 AT&T가 3-스크린 플레이라는 개념을 주창하여 TV, PC, 휴대전화를 인터넷으로 연결해 콘텐츠를 동기화하여 콘텐츠의 OSMU(One Source Multi Use) 서비스를 제공하고자 하는 발상에서 시작되었다. OSMU란 사용자가 구입한 콘텐츠를 사용자가 가지고 있는 기기 내에서 자유롭게 이용하는 것으로 N-Screen은 OSMU를 실현할 수 있는 하나의 해결책으로 떠오르게 되었다.

2) 법·제도

(1) 국내 N-Screen 관련 법률

현재 N-Screen과 관련된 법령은 활용 분야에 따라 크게 플랫폼, 서비스, 콘텐츠 관련 법령으로 구분할 수 있다. 플랫폼에 관련된 법률로는 전자기기에 적용될 수 있는 전파법, 전기사업법 등 통신 인프라에 관련된 법률이 있고, 서비스에 관련된 법률로는 방송법, 전자서명법 등의 IT 서비스와 관련된 법률이 있다. 또한 콘텐츠에 관련된 법률로는 스마트 디바이스를 통해 제공될 수 있는 멀티미디어 콘텐츠에 관한 법률 및 지적 재산권에 관련된 법률을 예로 들 수 있다. 다음 [표 1]은 N-Screen을 구성하는 카테고리별로 적용될 수 있는 법률을 정리한 것이다.

[표 1] 국내 N-Screen 관련 법률

구분	관련법령	
플랫폼	• 전기통신기본법 • 전기통신사업법 • 정보통신공사업법 • 정보시스템의 효율적 도입 및 운영 등에 관한 법률	• 전기사업법 • 정보통신산업진흥법 • 정보통신망 이용촉진 및 정보보호등에 관한 법률 • 전파법
서비스	• 방송법 • 인터넷 멀티미디어 방송사업법 • 인터넷주소자원에 관한 법률	• 전자거래기본법 • 전자서명법
콘텐츠	• 콘텐츠산업 진흥법 • 지식재산기본법 • 저작권법 • 온라인 디지털콘텐츠 산업 발전법	• 이러닝산업발전법 • 게임산업진흥에관한법률 • 음악산업진흥에관한법률 • 영화 및 비디오물의 진흥에 관한 법률

(2) 국외 N-Screen 관련 법률

국내 뿐 아니라 국외에서도 N-Screen에 관한 사항은 현재 표준화 및 관련 기술이 연구 단계에 머물러 있어 N-Screen 환경에 특화된 법령은 제정되지 않은 상태이다. 국가별로 기존에 제정된 법령을 기준으로 N-Screen 서비스에 있어 적용할 수 있는 법률은 다음 [표 2]와 같이 정리할 수 있다.

[표 2] 국외 N-Screen 관련 법률

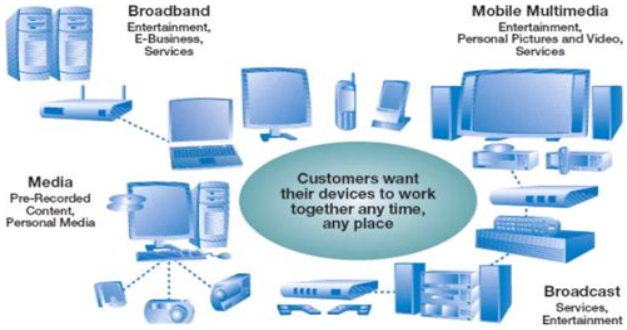
국가	관련법령	
미국	• 고성능 컴퓨팅 및 통신법 • 국내외 상거래에 있어서의 전자서명법 • 정보자유법 • 저작권문제 정리, 명확화 및 수정에 관한 법	• 통신법 • 케이블 통신법 • 무선통신과 공공안전법 • 전자행정법 • 인터넷방송 조정법 • 케이블 TV법
일본	• 전파법 • 방송법 • 유선전기통신법 • 전자서명 및 인증업무에 관한 법률 • 지적재산기본법 • 저작권법	• 고도정보통신네트워크 사회형성 기본법 • 유선텔레비전 방송법 • 표준텔레비전방송에 관한 송신의 표준 방식 • 전기사업법
유럽	• 디지털 경제활동법 • 무선통신법 • 전자등록법 • 무선전신법 • 정보서비스법	• 저작권법 • 모바일전화법 • 전기통신법 • 방송법

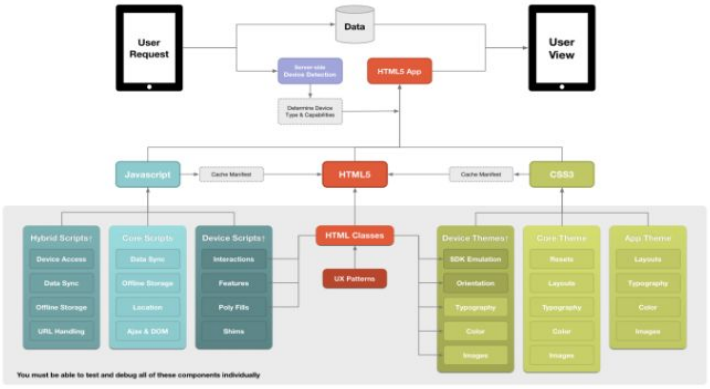
3) 기술

N-Screen을 구성하는 요소 기술은 활용 분야에 따라 법률과 마찬가지로 크게 플랫폼, 서비스, 콘텐츠의 세 가지 분야로 나눌 수 있다. 각각의 분야에 따라 상이한 기술들이 적용되어 연동될 수 있다. N-Screen 서비스 및 콘텐츠의 제공을 위해 각 분야에 적용되는 구체적인 세부 기술들은 다음의 [표 3]과 같이 정리할 수 있다.

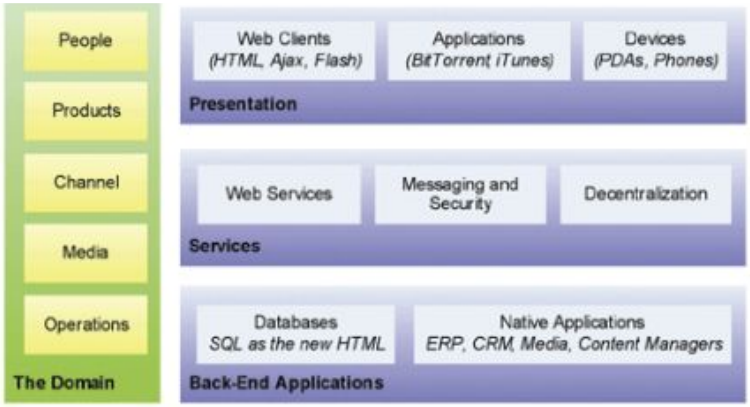
[표 3] N-Screen 관련 기술

구분	관련 기술	상세
플랫폼	클라우드 컴퓨팅	- 인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 IT자원들을 '서비스'로 제공하는 컴퓨팅. [3] - 표준화된 IT 기반 기능, IP망을 통한 접근, Always on과 수요에 따른 확장성 지원, 사용량이나 광고 기반 과금, Web 혹은 Programmatic 기반 Control Interface, 사용자 셀프 서비스 등의 특성을 지님. - 서비스의 대상과 범주에 따라 Public Cloud, Private Cloud, Hybrid Cloud 등으로 분류하기도 하며, 제공되는 형태에 따라 SaaS, AaaS, Paas, Iaas등으로 분류하기도 함. [4]  [그림 3] 클라우드 컴퓨팅 개요도
	DNLA	- Digital Living Network Alliance의 약자로, 본 기술 인증을 받은 제품 간에는 다양한 미디어 콘텐츠의 자유로운 공유 및

<table>
<tr><td></td><td></td><td>재생이 가능하도록 하는 전송 및 공유 규격. [5]
- 콘텐츠별 다양한 확장자의 호환을 지원하여 다양한 모바일 및 가전 기기 간의 콘텐츠의 이동 및 재생을 용이하게 하여 N-Screen 및 홈 네트워크를 구성하는 기반 기술.
 

[그림 4] DLNA 구성도</td></tr>
<tr><td rowspan="2">서비스</td><td>HTML5</td><td>- HTML의 차기 주요 제안 버전으로 웹 브라우저 벤더의 주도로 표준화가 이루어지고 있는 월드 와이드 웹의 핵심 마크업 언어. [6]
- 다양한 멀티미디어 콘텐츠, 데이터베이스의 연결 및 양방향 통신을 위한 태그 및 API등의 지원을 통해 멀티미디어 콘텐츠에 특화된 서비스 및 이기종 다매체 환경의 지원을 위한 요소를 포함. [6][7]
 

[그림 5] HTML 구성도</td></tr>
<tr><td>Web 2.0</td><td>- 모든 사람이 제공되는 데이터를 활용하여 다양한 신규 서비스를 생산해 낼 수 있는 플랫폼으로서의 웹 환경으로, 참여, 공</td></tr>
</table>

		유, 개방의 개념을 통해 사용자가 새로운 서비스를 창출하고 리드하는 특성을 가짐. [8] - XML, Open API, AJAX등의 웹 표준에 기반한 클라이언트 확장 기술을 기반으로 다양한 디바이스와 네트워크 환경에서 통합적인 서비스 지원을 위한 표준화 진행중.  [그림 6] Web 2.0 아키텍처
	스트리밍	- 웹 상에서 실시간으로 음악 및 비디오 등의 멀티미디어 콘텐츠를 전송하고 재생하기 위한 기술. - 현재 웹 환경에서는 Progressive Download, RTMP/RTSP Streaming, Adaptive HTTP Streaming등의 방법이 이용되고 있음.
콘텐츠	**DRM**	- 웹을 통한 다양한 콘텐츠(전자책, 음악, 비디오, 게임, 이미지 등)의 안전한 배포를 보장하고, 불법 복제 및 결제 대행 등 콘텐츠의 생성 및 전송 관리를 지원하여 저작권을 보장하는 기술. [9] - 디지털 홈 DRM(CAS,DRM), 스트리밍 콘텐츠용 DRM (ISMACryp, VOD 지원 DRM, 멀티캐스트 지원 DRM) 등으로 구분. [09][10]
	멀티 미디어 압축 기술	- 스트리밍 및 기타 서비스의 제공 시 콘텐츠의 빠르고 원활한 전송과 안정적인 이용을 위해 대용량 멀티미디어 데이터의 품질을 보장하며 용량을 최소화하기 위한 기술.[11] - 텍스트(txt, doc, hwp 등) 이미지(jpeg, bmp, png, gif 등), 오디오(mp3, wma, aac, m4a 등), 비디오(avi, mp4, m4v, ts, wmv 등)의 확장자 범주로 구분.

2. 개인정보

1) 개요

개인정보란 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아 볼 수 있는 것을 포함한다)”를 말한다. 즉, 본인의 의사에 반하거나 본인이 알지 못하는 상태에서 이용될 경우 정보 주체(혹은 당사자)의 안녕과 이해관계에 영향을 미칠 수 있는 개인 관련 정보는 모두 개인정보라고 할 수 있다.[12]

개인정보를 유형별로 정리하면 다음 [표 4]와 같다. 현행되고 있는 개인정보는 주로 개인의 신상 및 개인의 관계성에 기반을 둔 정보가 대부분이다.

[표 4] 일반적 개인정보의 유형과 종류

유형 구분	개인정보의 종류
일반 정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 성별
가족 정보	가족구성원들의 이름, 출생지, 생년월일, 직업, 전화번호
교육 정보	학력 사항, 기술자격증 및 전문면허, 상벌 사항
병역 정보	군번 및 계급, 제대 유형, 주특기, 근무부대
부동산 정보	소유 주택, 토지, 자동차, 기타 소유 차량, 상점 및 건물 등
동산 정보	보유현금, 저축 현황, 현금카드, 주식, 채권, 예술품, 보석
소득 정보	현재 봉급, 봉급 경력, 보너스 및 수수료, 이자소득, 사업소득
기타수익 정보	보험 가입 현황, 회사의 판공비, 퇴직 프로그램
신용 정보	대부잔액 및 지불상황, 저당, 신용카드, 압류 통보 기록
법적 정보	전과기록, 자동차 교통위반기록, 구속기록, 이혼기록, 납세
의료 정보	가족병력기록, 과거의료기록, 정신질환기록, 각종 의료정보
신체 정보	지문, 홍채, DNA, 신장, 가슴둘레 등

이러한 정의가 담아내는 개인정보의 범위는 고정되어 있는 것이 아니라 지속적으로 확대되고 있다. 지식정보사회의 발달과 더불어 전자우편 주소, 신용카드 비밀번호, 로그파일, 쿠키(cookies)정보, 위치 정보, DNA 정보 등 새로운 개인정보가 계속 등장하고 있다.

국내 뿐 아니라 세계 각국의 법률에 정의되어 있는 개인정보 또한 공통적으로 '개인에 관한 정보(Personal Data)'를 말하고 있으며, 개인정보는 식별된 또는 식별가능한 개인에 대한 정보라고 정의할 수 있다. 구체적인 개인정보 관련 해외규범에서의 정의는 [표 5]와 같이 정리할 수 있다. [12]

[표 5] 개인정보 관련 해외규범에서의 정의

주체/출처	내용
OECD/개인정보 가이드라인	- 식별된 또는 식별 가능한 개인(정보 주체)에 관한 정보
EU/1995 개인정보 보호 지침	- 식별된 또는 식별 가능한 자연인(정보 주체)에 관한 정보. 단, 식별가능한 사람은 특히 신원증명번호 또는 육체적·심리적·정신적·경제적·문화적 또는 사회적 신원 중 하나 이상의 요인을 참고하여 직접적 또는 간접적으로 식별될 수 있는 사람을 말함
홍콩/개인정보법	- 생존하는 개인에게 직접적 또는 간접적으로 관련되어 있고, 직접 또는 간접적으로 개인의 신원을 확인하기 위하여 이용할 수 있으며, 해당 정보에 대한 접근이나 처리가 이루어질 수 있는 형태의 정보
일본/개인정보의 보호에 관한 법률	- 생존하는 개인에 관한 정보로서 당해 정보를 포함하는 성명, 생년월일, 기타 기술 등에 의해 특정한 개인을 식별하는 일이 가능한 정보(다른 정보와 용이하게 결합하여 그에 의해 특정한 개인을 식별하는 것이 가능한 경우도 포함)
영국/정보보호법	- 해당 정보 또는 해당 정보와 정보 관리자가 소유하거나 소유하게 될 다른 정보를 결합하여 식별될 수 있는 생존 개인에 대한 정보
캐나다/ 프라이버시법	- 기록된 형태에 관계없이 식별 가능한 개인에 관한 정보

2) 법·제도

(1) 국내 개인정보 보호 관련 법률

2011년 9월 30일자로 개인정보를 관할하는 법률인 「개인정보 보호법」이 시행되었다. 개인정보 보호법은 개인정보의 수집과 유출, 개인정보의 오·남용으로부터 사생활과 권리를 보호하기 위해 제정된 법이자 공공 및 민간부문을 모두 포함하는 개인정보에 관한 일반법이다. [13]

새롭게 개정된 개인정보 보호법을 시행함으로써 공공부문과 민간부문의 개별적 법률 적용을 통합적으로 변경하고, 법의 적용 대상 및 적용 범위를 확대하여 전자 파일 형태로 기록된 개인정보 뿐 아니라 서면으로 수집된 개인정보에도 본 법령을 적용하여 법적용 사각지대를 해소하는 데 의의를 둔다.

또한, 주민등록번호 등 고유식별번호의 처리를 엄격히 제한하고, 영상정보처리기기(CCTV) 설치·제한에 대한 근거 규정을 마련하며, 개인정보 영향평가를 도입하는 등 개인정보 침해사고 예방과 국가의 개인정보보호 수준을 획기적으로 강화한다. 마지막으로 개인정보에 대한 사용자의 권리가 강화되어 정보 주체가 수집된 자신의 개인정보를 손쉽게 열람·수정 및 처리정지권을 보장하며, 개인정보 침해 사고 발생 시 분쟁 조정을 위한 절차가 간소화되고 용이해 졌다는 특징을 지니고 있다.

(2) 국외 개인정보 보호 관련 법률

세계 각국의 개인정보 보호 법률 체계는 크게 유럽식 모델(일원적·포괄적 규제)과 미국식 모델(이원적·부문별 규제)로 구분되어 있다. 유럽 각국의 개인정보 보호법은 사회 전 분야에 걸친 수집·이용 원칙, 정보주체의 열람·정정권, 집행·감독기구 등 포괄적 기준(캐나다, 호주 등도 유럽식 모델과 유사)을 규정하고 있다. [표 6]는 국외 개인정보 보호 관련법 현황을 정리한 것이다.[14]

[표 6] 국외 개인정보 보호 관련법 현황

국가	법률명 및 시행 시기
영국	정보보호법 (1998)
프랑스	정보처리파일 및 자유에 관한 법률 (1978)
독일	연방정보보호법 (1994)
스웨덴	개인정보법 (1998)
스페인	개인정보 보호기본법 (1999)
네덜란드	개인정보 보호법 (1999)
일본	개인정보 보호법(2005)
미국	프라이버시법 (1974), 컴퓨터에 의한 정보조합과 프라이버시보호에 관한 법률 (1988), 건강보험책임법

미국은 공공부문의 경우 「프라이버시 보호법(Privacy Act)」 등 법률을 통해 엄격히 규율하고 있는 반면, 민간부문은 법률을 통한 규제보다 시장 자율규제에 중점을 두고 있다. 민간부문의 개인정보 보호법은 의료, 운전면허, 비디오 대여, 아동 프라이버시 등 특정 영역에 한하여 입법되고 있다.

EU는 개인정보보호를 위해 필요에 따라 부분별 입법화를 하기 보다는 적극적으로 전체를 포괄할 수 있는 일반적 원리들을 규정하고 있다. 유럽 국가들은 정보보호 활용 제도로 1995년에 제정된 유럽 공동체 개인정보 관리 지침(EU Directive)을 기본으로 삼아 각국의 사정에 따라 수정 및 보완된 것을 사용하고 있다. 유럽 각국에서는 개인정보를 수집하고 이를 이용할 경우 사전 동의 혹은 사후 동의를 의무화 하고 있다.

일본은 개인정보 대량 유통, 유출 사건의 급증 및 프라이버시의 권리 개념 변모에 의한 필요성에서 2005년 개인정보보호법을 제정하고 시행하였다. 주로 EU의 개인데이터보호지령과 OECD 프라이버시 가이드라인을 참고하여 작성된 것이 특징이다.

3) 기술

(1) 개인정보 침해 대응 기술

개인정보 침해 기술(Privacy Invading Technology : PIT)은 컴퓨터 환경 내 개인정보 관련 오·남용 또는 악의의 피해가 발생할 수 있는 분야에 대하여 기술적 관점에서 체계적으로 분석하고 대응할 수 있는 기술적 체계 구성을 말한다. 주 내용은 [표 7]과 같다. [16][17]

[표 7] 개인정보 침해 기술 분석표

침해대응기술	방 법
TCP/IP 주소	• TCP/IP 주소의 분배 및 관리 체계 특성 때문에 인터넷 이용 시 TCP/IP 주소를 추적하여 이용자 신원을 확인하는 것이 용이
도메인 네임	• e-mail의 출처를 확인하는 것은 매우 간단하며, 누구나 ISP 정보와 e-mail 사용자의 ID를 알 수 있음 • ISP는 이용자의 ID를 이용하여 계정의 확인이 가능
Processor Serial Number(PSN)	• IntelⅢ 침에 고유의 프로세서 일련 번호를 부여하여, 인터넷에 접속하는 특정 컴퓨터 이용자의 신원정보와 연결시켜 전자상거래에서 인증 목적으로 이용
IPv6	• IPv6의 계획은 인터넷의 모든 장치에 고정된 주소를 할당하는 것 • IPv6의 새로운 주소는 하드웨어 속에 내장되고, 추적 가능한 정보를 포함하게 된다. 이것은 마치 영구적인 쿠키를 심는 것과 동일한 개념
쿠키	• 쿠키 파일을 이용하여 인터넷 이용자의 신원을 쉽게 파악 가능 • 로그인 정보 및 기타 중요 정보등의 로드가 가능 • 쿠키에 담긴 정보를 통해 마케팅 데이터베이스에 있는 이용자의 이름, 주소, 이전의 소비정보등을 상호 비교함으로써 사용자의 신원 확인이 용이
웹을 통한 유출 (버그, 피싱, Malware)	• 웹 버그는 온라인 이용자가 모르는 사이에 이용자에 관한 정보를 유출하거나 심지어 이용자의 시스템을 파괴할 수 있는 기술

스파이웨어	• 무료 또는 유료로 배포되는 소프트웨어에 들어 있는 일종의 프로그램 모듈을 통칭 • 해당 소프트웨어를 설치한 컴퓨터 이용자가 인터넷을 서핑할 때 이용자의 개인정보나 온라인 활동 정보를 스파이웨어를 설치한 회사의 서버에 지속적으로 전송하는 것이 주된 기능
고성능 스파이웨어 기술	• 스파이웨어를 탐지하기 위해 사용되는 백신이나 안티 스파이웨어 솔루션 등을 우회하기 위해 수집된 정보를 작은 크기로 나누어 컴퓨터 파일시스템의 보이지 않는 틈새 공간(slack space)에 임시 저장한 다음, 특정 시간대의 내·외부의 특정인에게 전송하는 방법을 이용
무선랜(WLAN) 환경	• WLAN 사용자가 액세스 포인트에 접속할 때 해커가 가상의 액세스 포인트를 이용하여 사용자의 중요한 개인정보를 모니터링하게 됨
웹메일의 첨부 파일 유출	• 기존 e-mail이나 웹메일을 모니터링 하여 데이터를 유출하는 방식에서 한 단계 진화 • 웹메일에 첨부된 파일을 encoding하는 방식으로 주로 기업이 운용하는 메일 모니터링 프로그램을 우회하여 기밀정보를 유출
스테가노그래피 (Stegenography)	• 이미지 및 오디오 파일에 중요한 파일이나 메시지를 첨부할 수 있는 스테가노그래피 기법이 확산될 전망
접속세탁 (Connection laundering)	• 해커들이 그룹간 공간 창조를 통해 해커 역추적 경로 파악을 어렵게 하는 것 • 여러 국가를 경유하여 해킹을 할 경우, 중간 단계의 해커 그룹이 운영하는 가명경로(anonimyzer)를 거쳐 해커에 대한 역추적이 불가능하게 하는 방법
위치측정 정보	• GPS, RFID 또는 휴대전화기의 위치 측정 내용을 인터넷을 통해 사용자 동의 없이 개인의 위치 정보가 유출되는 방법

(2) 개인정보 강화 기술

개인정보들이 사용자 동의 없이 유출되는 것을 막기 위한 방법 중 대표적으로 사용되는 기술, 즉 사용자의 정보가 빠져나가는 것을 막는 PET(Privacy Enhancing Technology) 기술은 다음 [표 8]과 같이 요약할 수 있다. [18]

[표 8] 개인정보 강화 기술 요약

분류	서비스	특징	기술
Web 기반 기술	Client의 익명성 제공	- 웹 사용자의 인터넷 이용에 관련된 정보를 숨기고 암호화를 통한 데이터 트래픽의 내용을 숨긴다.	• Anonymizer • Onion Routing • Crowds
	Server의 익명성 제공	- URL 암호화를 통한 익명성을 제공하고 브라우저의 암호화, 데이터 스트림의 암호화를 통한 데이터의 무결성 및 보안을 제공한다.	• Janus
Network 기반 기술	네트워크에서 정보의 안전성과 신뢰성 제공	- 접근제어, 침입탐지, 침입차단, 패킷 및 침입 경로 추적 암호화와 복호화, 인증을 통해 안정성을 제공한다.	• 프록시 • Firewall • IDS • IPS
Agent 기반 기술	인터넷의 정보 유출에 대해 사용자를 대신하여 통제	- 다른 소프트웨어와는 다르게 에이전트는 스스로 판단하여 행동하는 자율성을 가진다.	• Cookie manager • Ad blocker • Spyware Filter

3. 기존 모델 연구

N-Screen 서비스와 관련된 연구는 기존에도 여러 논문을 통해 발표된 바 있다. 그러나 기존에 제시된 논문은 환경의 제약 및 한정적인 본 논문에서는 기존에 제시되었던 N-Screen 서비스 관련 논문을 분석하고 제시하고자 하는 모델과 비교함으로써 제시하는 모델의 효율성을 가시화한다.

1) DNLA 기반 콘텐츠 공유 및 동기화 모델

본 모델에서는 홈 네트워크 환경에서 DLNA 및 UPnP 기술을 기반으로 N-Screen 관련 서비스 모델[19]을 제안하였다. 홈 네트워크를 구성하는 기술 중 하나인 미들웨어 기술을 이용하여 홈 네트워크를 구현하고, 또 미들웨어 기술 내부에 포함되어있는 UPnP(Universal Plug and Play)기술을 이용하였다.

UPnP기술은 IP 기반으로 이기종 플랫폼을 지원할 수 있도록 하는 기술로, 해당 모델에서는 이 기술로 이기종 다매체 기기에 콘텐츠를 전송할 수 있도록 하였다. 해당 기술을 이용하여 컨트롤 포인트와 디바이스의 제어 그리고 미디어 관리까지 함께 수행하고, 유·무선 네트워크를 동시에 지원할 수 있다.

또한 DLNA 3-Box 모델을 차용하여 콘텐츠의 원활한 지원을 구현하였다. DLNA 3-Box 모델은 크게 DMC(Digital Media Controller), DMS(Digital Media Server), 그리고 DMR(Digital Media Render)로 구성된다.

모델 내부의 흐름은 크게 다음과 같다. DMC에서는 네트워크 상에 존재하는 디바이스들을 식별하고 디바이스들의 정보는 DMC에 저장이 된다. DMC에서 DMS에게 정보를 요청하여 열람하고, 해당 정보에서 사용하고 싶은 콘텐츠의 재생을 요청하게 된다. 이때 사용자는 DMC를 통해 콘텐츠를 재생할 디바이스(DMR)를 선택할 수 있다. 콘텐츠 재생 요청이 끝난 DMR에서는 콘텐츠를 저장하고 관리하는 DMS에게 콘텐츠의 전송을 요청하여 A/V 스트리밍을 통해

콘텐츠를 전송받게 된다.

본 모델은 DLNA기술을 통해 해당 인증을 받은 디바이스라면 DLNA 3-Box 모델을 통해 이기종 다매체 환경에서 콘텐츠를 원활히 제공받을 수 있다는 이점이 있지만, DLNA 인증을 받지 않은 기기를 사용하는 경우에는 콘텐츠의 이용이 어렵다는 점이 있고, 또한 이용하고자 하는 디바이스에서 직접 콘텐츠의 재생을 선택하는 것이 아니라 특정 PC에 구현되어 있는 DMC를 통해 재생하고자 하는 디바이스를 선택해야 하는 불편함이 있다. 또한 이기종 다매체 환경을 지원한다고 기술하였으나, 프로토타이핑에서 미루어 보았을 때 다양한 OS 환경이나 기기를 지원한다고는 보기 어려운 점이 있다. 마지막으로 이와 같은 N-Screen 서비스를 제공하는 데 있어 콘텐츠 혹은 개인정보의 보안과 관련된 사항은 고려하지 않고 단순 콘텐츠의 전송만을 구현했다는 단점이 있다.

2) HTML5 기반 서비스 세션 이동 모델

본 모델에서는 HTTP 스트리밍 환경에서 스트리밍 서비스 세션 이동성을 보장할 수 있는 N-Screen 관련 서비스 모델[20]을 제시하였다. 현재 표준이 이루어지고 있는 HTML5 기반 적응적 HTTP 스트리밍 환경에서 서비스를 지원하고 자바스크립트 언어를 통해 미디어 및 세션 제어를 할 수 있도록 구현하였다.

네트워크 대역폭 변화에 적응적으로 대응하기 위해 콘텐츠를 여러 압축률로 압축한 파일을 네트워크 상태 변화에 따라 전송을 최적화 하는 HTTP 기반 스트리밍 기술을 차용하여 단말간 세션 이동 메커니즘을 통해 단말간 서비스 연속성을 보장한다.

사용자가 서비스 세션 이동을 하기 위해서는 단말 간 서비스 이용 시 필요한 정보와 세션 정보를 주고 받을 때 사용자 식별과 개인 세션정보의 보호를 위해

세션 제어 서버로의 사용자 관리 정보를 전송해야 한다. 또한 사용자가 오프라인인 경우 세션 정보 관리를 위해 로그인 정보 관리도 필요하다. 전송되는 정보로는 사용자 ID, 콘텐츠의 주소, 현재 재생 시점, 콘텐츠 이름, 세션을 전달받는 사용자의 ID, 전달 시간 등이 있다.

메커니즘의 기본 원리는 다음과 같다. 사용자가 서비스 세션을 이동하고자 할 때 메커니즘 내에서 콘텐츠의 주소와 현재 재생 시점을 변경하고자 하는 사용자 혹은 기기에 전송을 하고, 변경 후 저장되어 있는 세션 정보를 로드하여 저장된 콘텐츠와 재생 시점을 불러와 연속성을 유지한다. 서비스 세션의 이동 방법에는 콘텐츠 사용자가 다른 사용자에게로 세션을 변경하는 방법과, 새로이 콘텐츠를 이용하려고 하는 사용자가, 현재 사용중인 사용자의 서비스 세션의 이동을 요청하는 방법이 있다.

본 모델은 HTML5 언어를 기반으로 콘텐츠의 연속성을 제공하고 세션을 변경할 수 있다는 점에서 다양한 기기 및 환경에 통합적인 적용이 가능하다는 장점이 있지만, 사용되고 있는 콘텐츠의 단순 이동에만 초점을 맞추어 사용자의 편의성을 고려한 부가 데이터 등의 제공이 부족하다는 단점이 있다. 또한 콘텐츠의 유해성 점검과 같은 콘텐츠 검증 과정이 포함되어 있지 않아 유해 콘텐츠가 유포될 수도 있는 가능성을 내포하고 있다. 마지막으로 사용자 및 기기 인증에 관련된 부분이 배제되어 있어 인가되지 않은 사용자 및 불법적인 기기에서의 서비스 전환에 있어 많은 보안적 부분의 위협이 발생할 가능성 또한 포함하고 있다.

Ⅲ. N-Screen 환경 내 콘텐츠 이용 문제점

N-Screen 환경이 확산되면서 이를 기반으로 하는 다양한 형태의 서비스 또한 그 이용률이 증가하는 추세이다. 새로운 환경에서의 혁신적인 서비스 및 대용량 멀티미디어 콘텐츠의 이용률이 증가하면서 이에 대한 문제점 또한 부각되고 있는 상황이다. 그 중에서 가장 크게 우려되고 있는 것이 다름 아닌 스마트 디바이스를 통한 개인정보의 유출로 인한 피해이다. 스마트 디바이스를 통한 개인정보의 유출을 통해 금전적인 피해 사례는 아직 보고된 바가 없지만 스마트 디바이스 환경의 확산 및 서비스 패러다임의 이동에 따라 앞으로 예상된다. 또한 개인정보의 유출을 우려한 사용자들의 소극적인 서비스 이용으로 인해 N-Screen 환경 내에서 콘텐츠의 이용이 원활하게 이루어지지 못한다는 점 또한 문제점으로 지적되고 있다. 다음은 N-Screen 서비스 환경 내에서 콘텐츠 이용 시 문제점으로 고려될 수 있는 사항들을 나타낸 것이다.

- ✓ **불법 콘텐츠의 유포로 인한 사용자의 불법 콘텐츠 오용**
- ✓ **기기 및 서비스 내 저장된 개인정보의 유·노출**
- ✓ **사용자 권한 관리의 부주의로 인한 권한 밖의 콘텐츠 이용**
- ✓ **다양한 제약으로 인한 N-Screen 환경 내 콘텐츠 이용의 불편**

모바일 기기에서의 OS의 도입에 따라 기존의 모바일 환경과는 또 다른 위협들이 등장 하였다. 이에 따라 인터넷 환경에서 배포되고 있는 콘텐츠가 내장하고 있는 위협 요소 뿐 아니라 스마트 디바이스가 내재하고 있는 보안 취약성 및 사용자의 부주의로 인해 예상치 못한 경로로 개인정보가 유·노출될 수 있는 가능성이 증가할 것으로 예상된다.

관련연구에서 언급한 기존 모델과 같은 경우, 적용 기술은 각각 다르나 N-Screen 서비스를 지원한다는 점에서는 크게 차이가 없다. 그러나 N-Screen 기반의 서비스에 중점을 두어 콘텐츠를 이용하면서 야기될 수 있는 개인정보 및 콘텐츠에 대한 안전성은 보장되어 있지 않다. 본 논문을 통해 제시하는 모델과 기존 모델을 비교 분석하면 다음 [표 9]와 같다.

[표 9] 기존 모델과의 비교 분석

특징	DLNA 기반	HTTP 스트리밍 기반	본 논문
기반 기술	DLNA	HTTP 스트리밍 /HTML5	HTML5
지원 환경	스마트폰, PC	스마트폰, PC	스마트폰, PC, 태블릿 PC
지원 콘텐츠 종류	비디오	비디오	텍스트, 오디오, 비디오, 이미지
콘텐츠 연속성 지원	○	○	○
사용자 인증	×	×	○
기기인증	×	×	○
콘텐츠 검증	×	×	○
콘텐츠 접근제어	×	×	○

○:지원 △:일부지원 ×:지원안함

기존의 모델들과 같은 경우, N-Screen에 관련된 이기종 다매체 환경 지원, 콘텐츠 연속성 지원과 같은 부분은 모든 모델에서 지원을 하고 있으나, 사용자 인증 및 기기인증, 콘텐츠의 안전성 검증 및 접근 제어와 같은 부분은 지원하지 않아서 N-Screen 환경 내에서 콘텐츠를 이용하는 데 있어 개인정보보호에 관한 부분이 많이 결여되어 있는 것을 알 수 있다. 따라서 본 논문에서는 이와 같은 N-Screen 서비스를 지원하는 데 있어 필수불가결적인 개인정보보호 및 콘텐츠 보안에 대한 부분에 중점을 두고 모델을 설계 및 구현하였다.

Ⅳ. NTCPM(N-Screen Trusted Content Provide Model)

1. 개요

제 3장에서 다루었던 바와 같이, N-Screen 구성 단말의 확산 및 이를 이용한 다양한 서비스 및 콘텐츠의 보급률이 높아짐에 따라 새로운 환경 및 서비스에서의 안전하고 원활한 콘텐츠의 이용 방안이 요구된다. 본 논문에서는 이러한 요구사항을 해결하기 위한 NTCPM(N-Screen Trusted Content Provice Model)의 설계를 제안한다. 본 모델을 통해 스마트 디바이스를 통해 제공되는 서비스를 이용하는 사용자들의 개인정보의 보호를 강화하고 다양한 멀티미디어 콘텐츠가 포함하는 위험성을 분석하여 이를 사전에 사용자에게 알림으로써 사용자가 콘텐츠를 선택적으로 이용할 수 있도록 하는 방안을 제공한다. NTCPM은 총 4가지 기능 제공을 통하여 N-Screen 환경 내에서 사용자가 안전한 콘텐츠를 이용할 수 있는 방안을 제안한다.

NTCPM의 4가지 기능은 다음 [표 10]과 같다.

[표 10] NTCPM의 세부기능 상세

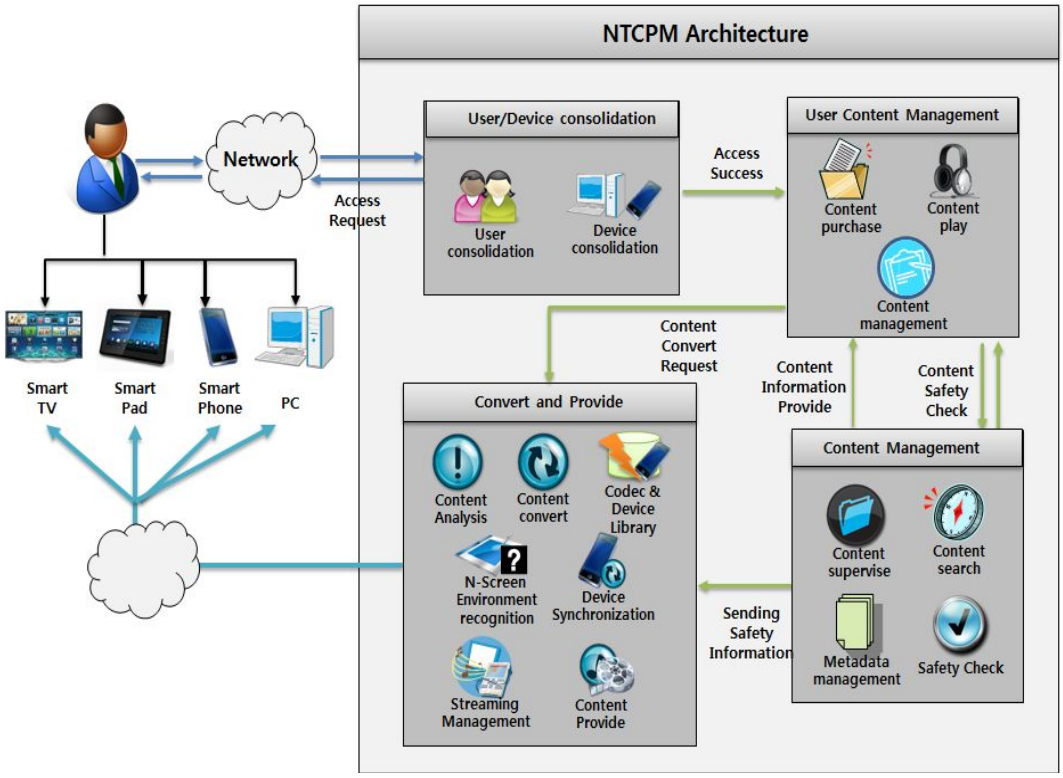
구성	상세
사용자/디바이스 인증	• 서비스를 이용하고자 하는 사용자의 신뢰성을 확인하는 사용자 인증 • 사용자가 접근하는 디바이스의 유효성을 확인하는 기기 인증
사용자 콘텐츠 관리	• 사용자가 서비스에 접속하여 각종 콘텐츠를 이용할 수 있도록 하는 기능으로, 콘텐츠의 구매 및 재생, 이용 내역의 기록 및 조회 기능 제공

콘텐츠 제어 및 안전성 검증	• 사용자가 이용하게 되는 콘텐츠의 기본적인 관리를 수행하는 부분으로, 콘텐츠의 등록, 수정 및 삭제, 콘텐츠의 검색 및 콘텐츠에 부가적으로 제공되는 메타데이터의 매칭 기능을 제공 • 다양한 콘텐츠에서의 개인정보 침해에 대한 취약점 혹은 위협으로 판단되는 요소를 체크하고 사용자에게 통지하는 콘텐츠의 안전성 검증 기능을 제공
콘텐츠 변환 및 배포	• 콘텐츠를 이용하고자 하는 기기 및 탑재된 OS를 파악하고 이들 기기로의 전송 및 이용 이에 적합한 형태로 콘텐츠를 가공 및 처리기능 제공 • 변환한 콘텐츠를 사용자의 기기로 전송하고 제어하는 기능을 제공 • 기기 변경에 따른 콘텐츠의 연속 재생 기능 제공

이와 같은 4가지 기능의 제공을 통해, 사용자가 보유하고 있는 디바이스의 OS 및 제조사에 종속되지 않고 콘텐츠를 자유롭게 이용할 수 있는 방안을 제공한다. 또한 콘텐츠의 안전성 검증 작업을 통해 N-Screen 환경 내에서 서비스를 이용하게 되는 사용자가 신뢰할 수 있는 콘텐츠를 편리하게 이용할 수 있도록 한다.

2. 구성

본 논문에서 제시하는 NTCPM에서 이루어지는 프로세스는 크게 3개의 세부 과정으로 구분할 수 있다. 1) 사용자 및 디바이스의 인증과 2) 요청 콘텐츠의 안전성 검증, 그리고 3) 변환 및 전송 과정으로 구성된다. 과정 1)에서는 접근을 요청하는 사용자가 시스템에 등록되어 있는지를 확인하고, 시스템을 이용하고자 하는 기기가 시스템 상에 등록이 되어 있는 것인지를 판단한다. 과정 2)에서는 사용자가 이용을 요청한 콘텐츠의 안전성을 분석하여 사용자에게 알린다. 과정 3)에서는 사용자가 이용을 승인한 콘텐츠를, 요청한 기기에 적합한 형태로 변환하고 전송한다. [그림 7]은 NTCPM의 전체 구성을 나타낸 것이다.



[그림 7] NTCPM Architecture

3. 기능

1) 사용자/디바이스 인증

(1) 사용자 인증

NTCPM에서는 허가되지 않은 사용자 및 디바이스의 접근을 제어하기 위해 사용자/디바이스 인증 과정을 거친다. 사용자의 인증은 NTCPM에 로그인을 하는 과정으로서 이루어지게 된다. 만약 등록되지 않은 사용자의 경우, NTCPM의 이용자로 등록하는 과정을 거친 후 로그인을 함으로써 이용 권한을 획득할 수 있다. 사용자 인증 과정에서는 서비스에 등록된 유저인지를 판단하고, 등록된 유저의 경우 로그인 상태로 전환하여 인증을 마친다. 또한 인증과정 중 사용자의 권한을 체크하여 접근 제어의 효과 또한 도모한다. 다음 [표 11]은 NTCPM에서 구분되는 사용자의 권한을 나타낸 것이다.

[표 11] 사용자 권한 상세

주 체		상 세
시스템 관리자		• 원활한 서비스의 제공을 위하여 시스템의 전반적인 관리를 수행하는 주체
사용자	콘텐츠 등록자	• 콘텐츠를 판매하고자 하는 사용자로서 주로 기업 사용자 혹은 콘텐츠 제작자가 이에 해당
	일반 사용자	• 시스템에 등록된 콘텐츠를 실질적으로 구매하고 이용하게 되는 사용자 • 미성년자와 성인으로 구분할 수 있음

위와 같은 권한 구분에 따라 사용자 등급 별로 보여지는 시스템의 화면 및 이용할 수 있는 기능 및 콘텐츠가 달라지도록 구분한다.

(2) 디바이스 인증

사용자 인증 과정을 거치고 나서, 사용자가 접근을 시도한 디바이스의 인증이 이루어지게 된다. 사용자가 접근을 시도하여 콘텐츠를 이용할 수 있는 디바이스는 사전에 사용자가 시스템에 등록한 디바이스로 한정된다. 만약 사용자가 시스템에 등록하지 않은 디바이스에서 인증 과정을 진행할 경우, 시스템에서는 사용자에게 등록되지 않은 디바이스라는 Notice를 준 후, 콘텐츠 이용에 제약을 가하게 된다.

디바이스 인증에서는 사전에 사용자가 등록한 디바이스의 MAC Address, 혹은 디바이스의 전화번호 및 모델 번호와 시리얼 넘버, 혹은 IMEI와 같은 정보의 조합을 통해 디바이스 인증을 진행한다. 다음 [표 12]는 디바이스 인증에 이용될 수 있는 정보들을 나타낸 표이다.

[표 12] 디바이스 인증 이용 정보

활용 정보	특 징
MAC Address	• 이더넷의 물리적인 주소로, 48비트 길이의 스트링 • 유동적인 IP Address와는 달리 개개의 디바이스의 식별이 가능
시리얼 넘버 + 모델번호	• 제조사가 지정하는 고유 디바이스의 모델 종류 및 고유의 시리얼 넘버의 조합을 통해 개별 디바이스의 식별이 가능
IMEI	• 국제 모바일기기 식별 코드로 15자리의 숫자로 구성 • MAC Address와 유사하여 고유 디바이스 식별이 가능

위와 같은 디바이스별 고유식별번호를 통한 인증을 통해 사용자가 루팅 혹은 탈옥[1]된 디바이스나 인증되지 않은 사용자 기기에서의 불법적인 콘텐츠의 이용을 제한하고 안전성을 도모할 수 있다.

1) 모바일 OS를 탑재한 모바일 기기에서 OS의 관리자 권한을 획득하는 것으로 보안상의 많은 위험을 야기하는 원인으로 알려져 있음

2) 사용자 콘텐츠 관리

NTCPM에서의 사용자 콘텐츠 관리는 다음과 같은 세 가지의 세부 항목으로 구성된다. 1) 사용자의 콘텐츠의 구매, 2) 사용자가 이용 가능한 콘텐츠의 내역을 보여주고 트래킹 및, 관리할 수 있도록 하는 기본적인 콘텐츠 관리 기능, 3) 접속한 기기에서의 콘텐츠의 재생 요청과 같은 기능을 지원한다.

(1) 콘텐츠 구매

먼저 사용자는 NTCPM에서 제공하는 콘텐츠 구매 기능을 통해 원하는 콘텐츠를 구매하고, 이를 이용할 수 있다. NTCPM에서 지원하는 콘텐츠는 주로 대용량의 멀티미디어 콘텐츠인 이미지, 비디오, 오디오 파일을 지원한다. 또한 콘텐츠는 무료 혹은 유료로 구분이 되어 있어 사용자가 구매를 한 후에 사용자의 콘텐츠 구매 리스트로 등록이 되어 관리될 수 있다.

(2) 콘텐츠 관리

사용자는 NTCPM에서 제공하는 콘텐츠를 사용자 콘텐츠 관리를 통해 제어하고 이용할 수 있다. NTCPM에서 구입한 콘텐츠는 사용자 보유 콘텐츠로 등록이 되어 사용자가 재생을 요청하거나 이용 내역을 파악하는 등의 다양한 관리를 수행할 수 있다. 콘텐츠 관리를 통해 사용자는 보유하고 있는 콘텐츠의 삭제 및 사용 기기의 제한 등의 부가적인 설정과 같은 기본적인 콘텐츠 관리 기능을 실행할 수 있다.

또한 시스템에 등록되어 있는 콘텐츠 이외의 사용자가 보유하고 있는 콘텐츠를 업로드하고 이에 대한 정보를 입력함으로써 시스템 내에서 자유로운 콘텐츠를 이용할 수 있도록 한다. 사용자가 업로드한 콘텐츠는 안전성 검증 과정을 거친 후 개인화되어 다른 사용자에게는 공개되지 않도록 한다.

(3) 콘텐츠 재생

사용자가 소유하고 있는 콘텐츠를 NTCPM에 등록되어 있는 유효한 디바이스를 통해 재생할 수 있도록 콘텐츠 변환을 요청하고, 기기로의 전송을 요청할 수 있다. 사용자가 이용할 수 있는 디바이스는 크게 모바일 OS를 탑재하고 있는 스마트폰, 스마트 패드, 스마트 TV가 대상이 될 수 있으나, 향후 모바일 OS를 탑재한 타 기기들의 이용이 증가하게 되면 충분히 확장될 수 있다.

사용자가 콘텐츠의 재생 요청을 하면, 이 요청은 콘텐츠 안전성 점검 기능 및 콘텐츠 변환 기능에 동시에 전달되어 콘텐츠의 검증 및 변환 작업이 이루어지게 된다. 콘텐츠의 재생은 기본적으로 모바일 OS 및 웹 브라우저에서 지원하는 기본 플레이어를 통해서 이루어지거나 별도의 뷰어 및 플레이어를 통해서도 재생될 수 있다.

(4) 콘텐츠 안전성 검증

콘텐츠 안전성 검증에서는 사용자가 이용을 요청한 콘텐츠 및 사용자가 업로드한 콘텐츠에 대한 안전성을 검증한다. 콘텐츠의 안전성을 검증하고 이를 사용자에게 통지함으로써 콘텐츠 이용의 안전성을 도모한다.

콘텐츠 안전성 검증은 크게 두 가지로 구분할 수 있다. 첫 번째로 내부에 사용자의 개인정보를 위협하는 요소를 검증함으로써 사용자의 개인정보를 보호하도록 한다. 콘텐츠에 포함 되어있는 개인정보 혹은 개인정보를 위협할 수 있는 요소들의 검증을 통해 안전성을 보장한다.

다양한 형태의 콘텐츠를 이용함에 있어 사용자가 이용을 요청하는 콘텐츠의 타입에 따라 검증되어야 하는 요소가 달라진다. 다음 [표 13]은 사용자의 개인정보 보호를 위해 콘텐츠 타입 별 검증 요소에 대한 상세 내용을 나타낸 것이다.

[표 13] 콘텐츠 타입 별 검증 요소

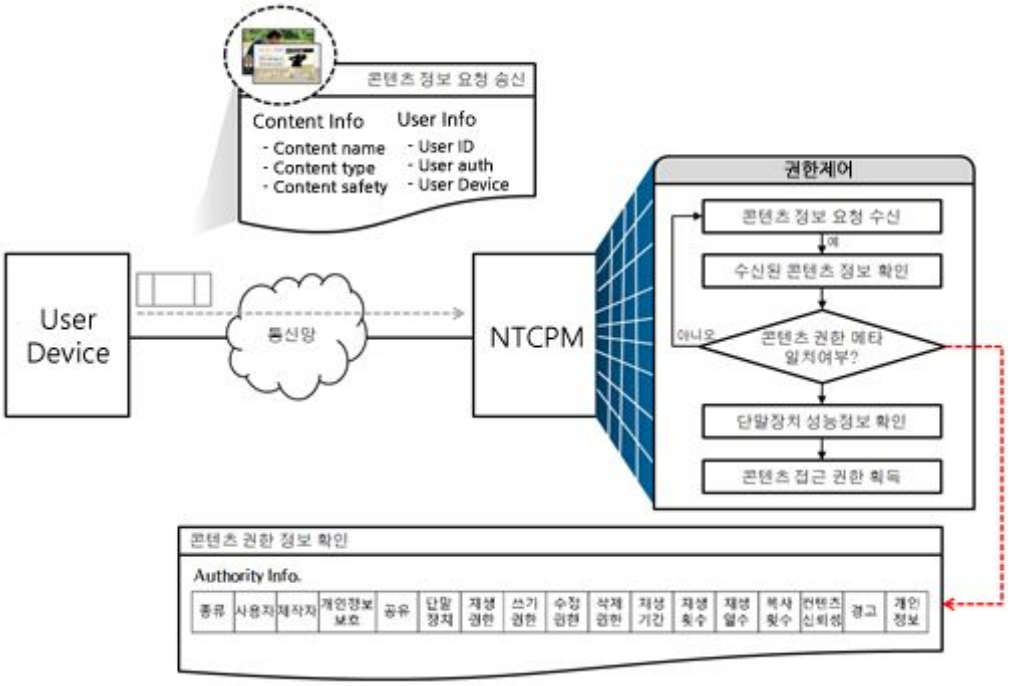
타입	검증 요소	검증 내역
텍스트	• 텍스트 내부에 포함되어 있는 개인정보로 예상되는 문자열(일정한 패턴을 가진 숫자 포맷, 특별한 포맷을 가진 문자열)	• 주민등록번호, 전화번호, 계좌번호, 카드번호 • 이메일 주소, 홈페이지 주소
이미지	• 이미지 파일 내부에 메타데이터와 흡사한 형태로 삽입된 바이러스 혹은 웜과 같은 유해요소 • 출처가 불분명한 콘텐츠 여부 • 불법 복제 콘텐츠 여부	• 바이러스 혹은 웜 감염 여부 • 메타데이터 내부 저작자 혹은 배포자 관련 필드
오디오 **비디오**	• 출처가 불분명한 콘텐츠 여부 • 불법 복제 콘텐츠 여부 • 유해콘텐츠 여부 • 인코딩 이용 코덱 안전성 여부	• 바이러스 혹은 웜 감염 여부 • 메타데이터 내부 저작자 혹은 배포자 관련 필드 • 인코딩 코덱 정보

두 번째로 사용자의 권한과 콘텐츠의 레벨을 비교함으로써 권한에 맞는 안전한 콘텐츠를 이용할 수 있도록 한다. 권한과 비교될 수 있는 콘텐츠의 레벨은 콘텐츠의 메타데이터나 태그에 기록되어 있는 정보를 이용할 수 있다. 콘텐츠의 레벨은 다음 [표 14]와 같은 기준을 통해 구분할 수 있다.

[표 14] 콘텐츠 레벨 분류

구분	선정성	폭력성	언어(대사)	공포	기타 (음주/흡연,약물)
Level 3	전신노출	살해	심한 비속어	충격적 공포	불법약물 표현
Level 2	부분노출	상해	거친 비속어	자극적 공포	약물 제한적 표현
Level 1	노출복장	격투(단순폭력)	일상 비속어	약간의 공포	약간의 음주/흡연
Level 0	노출없음	폭력없음	비속어 없음	공포심 없음	음주/흡연 없음

위와 같은 기준을 통해 콘텐츠에 입력되어 있는 정보를 판별하여 콘텐츠의 레벨을 정하도록 한다. 콘텐츠의 레벨이 정해지게 되면, 요청한 사용자의 권한과 비교하여 이용이 가능한 사용자인지를 판별하도록 한다. 다음 [그림 8]은 콘텐츠의 권한 확인을 수행하는 일련의 프로세스를 나타낸 것이다.



[그림 8] 콘텐츠 권한 제어 수행

3) 콘텐츠 관리

콘텐츠 관리는 크게 1) 콘텐츠의 등록, 삭제, 정보 수정과 같은 기본적인 기능을 수행하는 콘텐츠 정보 관리, 2)콘텐츠에 부가적으로 첨부될 수 있는 메타데이터의 관리, 3) 사용자에게 제공될 콘텐츠를 검색하는 콘텐츠 검색과 같은 기능으로 구성되어 있다.

(1) 콘텐츠 정보 관리

콘텐츠 관리는 콘텐츠를 등록하고자 하는 주체라면 이용이 가능하나 사용자의 권한에 따라 등록할 수 있는 정보가 달라진다. 다음 [표 15는] 시스템 사용 주체 별로 등록할 수 있는 정보를 정리해 놓은 것이다.

[표 15] 이용 주체별 등록 가능 정보

이용 주체	등록 가능 정보
관리자	• 콘텐츠 기본 정보(콘텐츠명, 콘텐츠 타입, 제작자, 저작권자, 콘텐츠 개요, 이용 가능 디바이스 등) • 이용자 관련 정보(이용 권한, 콘텐츠 이용 등급 등) • 콘텐츠 거래 정보(콘텐츠의 가격, 구매 후 이용 제한 날짜 등)
콘텐츠 등록자	• 콘텐츠 기본 정보(콘텐츠명, 콘텐츠 타입, 제작자, 저작권자, 콘텐츠 개요, 콘텐츠 등급 등) • 콘텐츠 거래 정보(콘텐츠의 가격, 구매 후 이용 제한 날짜 등)
일반 사용자	• 콘텐츠 기본 정보(콘텐츠명, 콘텐츠 타입, 콘텐츠 설명 등)

(2) 콘텐츠 검색

사용자의 콘텐츠 이용의 편리성을 증대하기 위해 NTCPM에 등록되어 있는 콘텐츠들을 다양한 분류로 검색할 수 있는 기능을 제공한다. 콘텐츠 등록 시에 데이터베이스에 등록 되었던 기본 정보를 통한 검색을 지원한다. 콘텐츠 이름을 통한 검색 외에도 콘텐츠의 타입별, 콘텐츠의 등급, 콘텐츠의 유/무료 여부와 같은 다양한 검색 조건을 통해 콘텐츠를 검색하여 손쉬운 사용을 도모한다.

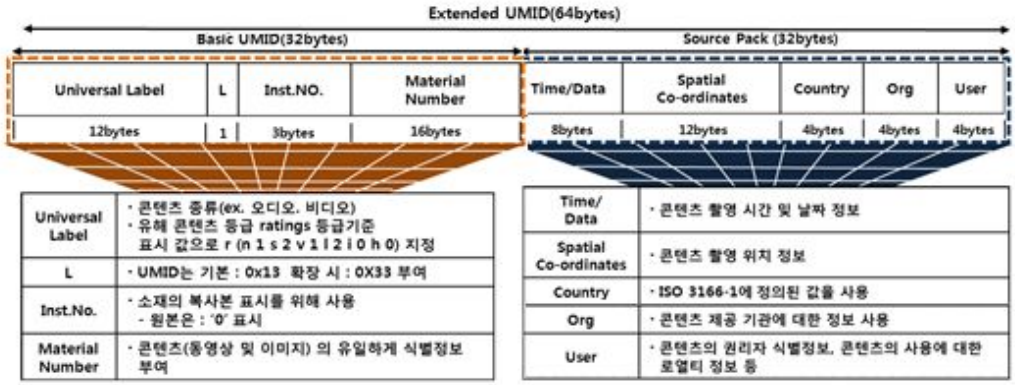
(3) 메타데이터 관리

NTCPM에서는 XML 형식을 통해 작성된 메타데이터의 등록을 통해 콘텐츠와 메타데이터를 연동 하는 것을 기본으로 한다. XML은 정보 작성 시 특정 웹 표준 및 정보의 입력 방식에 구속되지 않고 확장성이 뛰어나며, 데이터의 등록과 구조화 및 파싱 등의 처리가 용이하기 때문에 메타데이터 제공 시 가용성과 상호호환성을 높일 수 있다는 장점을 가지고 있다. 다음은 XML 형태로 작성된 메타데이터의 예시이다.

```
<?xml version="1.0" encoding="UTF-8"?>
<ProgramInformationTable>
    <ProgramInformation programId="crid://hbc.com/lovestory/lovestory">
        <BasicDescription>
            <Title type="main">
                Love Story
            </Title>
            <Synopsis>
                명문 부호의 아들인 올리버와 이태리 이민 가정의 가난한 제니는 사회적 신분의 차이를 극복하여..
            </Synopsis>
            <Keyword>love</Keyword>
            <Keyword>story</Keyword>
            <Genre herf="urn:mve:metadata:cs:FormatCS:3.5.7.3" type="main" />
        </BasicDescription>
        <OtherIdentifier>guid://e41a-b456-a876-3e49</OtherIdentifier>
        <OtherIdentifier>urn:mp4:DRMetadataStandard:diid:v-isan:
            29ef-94ba-53c4-3e7a-4ce8-e-5a45-98ec-f
        </OtherIdentifier>
        <MemberOf crid="crid://hbc.com/foxes/all" index="11"
            xsi:type="EpisodeOfType" />
    </ProgramInformation>
</ProgramInformationTable>
<GroupInformationTable>
    <GroupInformation groupId="crid://hbc.com/lovestory/all">
        <GroupType xsi:type=" ProgramGroupTypeType " value="movie" />
        <BasicDescription>
            <Title type="main">Melo Drama</Title>
            <Synopsis>또 다른 멜로 영화</Synopsis>
            <Keyword>Melo</Keyword>
            <Keyword>Love</Keyword>
            <Genre href="urn:tva:metadata:cs:FormatCS:3.5.7" type="main" />
        </BasicDescription>
        <MemberOf xsi:type="MemberOfType" crid="crid://hbc.com/movie" />
    </GroupInformation>
</GroupInformationTable>
```

[그림 9] XML로 작성된 메타데이터 형식 예제

또한 메타데이터의 필드의 분석을 통해 콘텐츠의 저작권 및 등급에 관한 부가 정보를 추출할 수 있다. 메타데이터를 구성하고 있는 정보의 표현 예시는 다음 [그림 10]과 같다.



[그림 10] 메타데이터 정보 표현 예시

또한 시스템을 통해 메타데이터를 등록하도록 하는 기능을 제공하여 콘텐츠 제공자 및 관리자가 메타데이터를 부가적으로 입력할 수 있도록 한다. 메타데이터를 입력받을 시에는 기본적인 형식을 제공하여 사용자에게 손쉬운 메타데이터 등록이 가능하도록 한다.

이와 같은 기능 제공을 통해 콘텐츠 제공 시 콘텐츠에 종속되는 메타데이터를 직접 등록하고 관리함으로써 콘텐츠 기본정보 뿐 아니라 부가적인 정보를 지원함으로써 콘텐츠 이용 시 다양한 정보를 제공할 수 있도록 한다. 단, 메타데이터의 관리와 같은 경우에는 PC만을 통해 등록하고 삭제도록 한다.

사용자 정의에 따라 메타데이터에 등록될 수 있는 정보는 콘텐츠의 타입을 기준으로 다음 [표 16]과 같이 나타낼 수 있다.

[표 16] 콘텐츠 타입 별 메타데이터 등록 정보

콘텐츠 타입	등록 가능 정보
이미지	• 파일명, 키워드, 구성 색상, 카테고리 등
오디오	• 곡명, 아티스트명, 장르명, 출시 년도, 수록 앨범명, 가사 등
비디오	• 영상명, 장르명, 출시 년도, 출연 아티스트, 줄거리 등

사용자가 입력한 정보를 바탕으로 NTCPM에서는 XML형태로 정보를 구조화하여 메타데이터로 사용할 수 있도록 변환한다. 이 때 사용자가 등록한 정보를 기준으로 콘텐츠의 안전성을 다시 한 번 검증하여 메타데이터 내에 콘텐츠의 레벨 및 안전성에 대한 정보를 추가할 수 있도록 한다. 다음 [그림 11]은 콘텐츠 메타데이터에 콘텐츠 레벨과 관련된 정보를 추가하는 예시이다.

```
<META http-equiv="PICS-label" content= '(PICS-1.1
"http://www.safenet.ne.kr/rating.html" l gen true for
"http://contentsprovider.com/adult" r (n 3 s 3 v 3 l 3 i 1 h 1))'>
<ContentInformationTable>
<ContentInformation
            contentsurl="http://contentsprovider.com/adult/episode1">
<ContentsDescription>
<Title type ="main">
   // 성인물 콘텐츠 제목
</Title>
<Keyword>// 성인물 검색을 위한 관련 키워드 삽입1</Keyword>
<Keyword>// 성인물 검색을 위한 관련 키워드 삽입2</Keyword>
</ContentsDescription>
<MaterialNumber>coutentsid://e41a-b456-a876-3e49</MaterialNumber>
<OtherIdentifier>urn:mpeg:mpeg21:diid:v-isan:
29ef-94ba-53c4-3e7a-4ce8-e-5a45-98ec-f
</OtherIdentifier>
</ContentInformation>
<ContentInformationTable>
```

[그림 11] 콘텐츠 레벨 정보 삽입 예시

4) 콘텐츠 변환 및 배포

콘텐츠 변환 및 배포는 크게 1) 콘텐츠 분석 및 변환과 2)단말 동기화 및 콘텐츠 전송 3)재생 중단 및 기기 변경으로 이루어진다. 사용자가 콘텐츠 이용을 요청하면 전달받은 콘텐츠를 사용자가 접근하고 있는 기기를 판별한 후 해당 환경에 맞게 변환한다. 변환 과정이 끝나게 되면, 사용자가 이용을 요청한 기기와 NTCPM의 동기화를 통해 전송하고 배포한다. 또한 사용자에게 콘텐츠를 배포할 때 콘텐츠의 전송 및 재생 시 수행하게 되는 스트리밍 서비스와 세션 및 기타 정보에 대한 제어·관리를 수행한다. 또한 N-Screen 환경에서의 재생 중단 및 기기 변경을 수행하고 관련 정보를 제어한다.

(1) 콘텐츠 분석 및 변환

콘텐츠 분석은 변환에 앞서 제공될 콘텐츠의 기본적인 정보를 파악하고 변환에 필요한 정보를 얻기 위해 이루어지는 과정이다. 사용자가 요청한 콘텐츠와 데이터베이스에 저장되어 있는 콘텐츠를 매칭 하여 콘텐츠의 유효성 여부를 확인한다. 콘텐츠 분석을 통해 콘텐츠의 타입, 콘텐츠의 확장자, 변환 가능한 파일 형식과 같은 정보를 추출하고 콘텐츠 변환 시 해당 정보를 참고하여 해당 콘텐츠에 적합한 변환이 이루어질 수 있는 사전 작업이 이루어질 수 있도록 한다.

콘텐츠 분석 과정을 통해 얻은 콘텐츠의 상세 정보 및 사용자가 이용하고자 하는 기기의 상세 정보를 연결하여 해당 기기에서 이용할 수 있는 형태로 콘텐츠를 변환하는 작업을 수행한다. 사용자가 선택한 기기의 종류 및 OS의 형태, 또는 콘텐츠의 타입에 따라 변환할 콘텐츠의 타입이 달라진다. 다음 [표 17]은 콘텐츠의 타입에 따라 이용될 수 있는 코덱 및 확장자를 나타낸 것이다.

[표 17] 콘텐츠 확장자 및 코덱 분류

콘텐츠 타입	분류	
	사용 가능 확장자	사용 가능 코덱(인코딩 방식)
텍스트	txt	UTF-8, EUC-KR, ANSI
이미지	jpg, png, bmp, gif	jpg, png, bmp, gif
오디오	wav, mp3, m4a, ogg, wma, flac	wav, mp3, m4a, ogg, wma, flac
비디오	asf, avi, ts, tp, wmv, mkv, mp4, WebM, OGV	영상 : H.264, DivX, Xvid, MPEG, avi, VP8, Theora 등 음성 : aac, avc, acc, Vorvis 등

콘텐츠 정보와 MAC Address 혹은 기기의 일련번호, IEMI 번호 등의 디바이스 정보의 분석을 통해 해당 디바이스에서 사용할 수 있는 콘텐츠의 확장자 정보를 얻고, 이에 적합한 코덱을 찾아 콘텐츠를 변환한다.

또한 콘텐츠 변환 시 콘텐츠 관리로부터 콘텐츠에 매치되어 있는 메타데이터를 전송받아, 이를 변환 되는 콘텐츠의 형태와 결합할 수 있도록 부가적으로 변환하고 콘텐츠에 포함하여 콘텐츠 내부에 포함되어 있지 않은 부가 정보를 전송할 수 있도록 한다. 기본적으로 상호호환성이 뛰어난 XML 형식의 파일을 이용하여 웹 브라우저 및 기타 환경에 종속되지 않고 이용할 수 있도록 한다.

(2)단말 동기화 및 전송

NTCPM에 접근하는 사용자가 현재 이용하고 있는 기기를 파악하여 정보를 추출하고 이 정보를 콘텐츠 변환 및 단말 동기화 과정에 이용한다. 단말 동기화와 같은 경우 단말의 유효성 및 가용성을 확인하고 콘텐츠를 안전하게 전송할 수 있는 세션을 확립하여 기기 및 OS에 맞는 스트리밍 서비스를 시작하기 위한 사전 준비와 같은 과정이라 볼 수 있다.

단말 동기화가 끝나면 사용자가 요청한 콘텐츠를 전송하게 된다. 이 과정에서

만약 사용자가 요청한 콘텐츠가 비디오 혹은 오디오와 같은 멀티미디어라면 NTCPM은 이들 콘텐츠를 스트리밍을 통해 서비스 하게 된다. 비디오 및 오디오 스트리밍 서비스 시 사용자 기기에 탑재 되어 있는 OS 및 사용 웹 브라우저 등을 판독해 해당 서비스에 가장 적합한 스트리밍 방식을 선택하게 된다. NTCPM에서는 현재 웹 환경에서 가장 보편적으로 쓰이고 있는 스트리밍 방식을 채택하여 스트리밍을 통해 서비스 한다. 이용할 수 있는 스트리밍 프로토콜은 다음 [표 18]과 같다.

[표 18] 이용 가능한 스트리밍 프로토콜

프로토콜	상세 내용
RTP	• 라우터 등의 통신망 기기에 의존하지 않고 단말기 간에 실행. • 수신 측에서 전송 지연이나 대역폭 등을 점검, RTCP를 사용해서 송신 측의 상위층 애플리케이션에 통지하는 것으로 부호화 속도 등을 조정하여 QoS 제어를 실현 가능.
RTCP	• 세션에 참가한 모든 참가자들의 전송상태에 대한 정보를 주기적으로 전송 • 최소한의 제어기능과 매체 식별기능을 제공하여 흐름제어가 가능.
RTSP	• 실시간으로 음성이나 동영상을 송수신하기 위한 통신 규약 • 스트리밍 시스템에 사용되며, 미디어 서버를 원격으로 제어할 때 사용. • RTP 규약을 사용해서 전송 계층으로 실제 오디오/비디오 데이터를 전송.

3) 재생 중단 및 기기 변경 제어

콘텐츠의 일시 정지 시 이를 감지하고, 사용자에게 기기 변경 여부를 체크하고 재생 이동을 수행한다. 사용자가 스트리밍 되는 콘텐츠를 일시정지 하거나 혹은 정지를 시도하였을 때 사용자에게 재생 지점 저장 여부를 물어 재생 중단이 확인되면, 타 기기에서 사용자가 콘텐츠를 이용할 때 재생 중단 지점에서부터 재생할 수 있도록 한다. 콘텐츠의 재생 중단 시점의 추출 및 중단 시점에서부터의 재생 기능은 HTML5, DOM(Document Object Model), Javascrip를

이용하여 실행한다. 다음 [표 19]는 콘텐츠 중단 시점 추출 함수의 예시이다.

[표 19] 콘텐츠 중단 시점 추출 함수

```
function pauseTime() {
//재생중인 콘텐츠 인식
 var playedContent =
            document.getElemenByTagName('video')[0];
//일시정지된 콘텐츠의 재생 중단 시점 추출
 var pausedTime = playContent.currentTime;
//콘텐츠와, 콘텐츠의 재생 중단 시점 저장
 savePausedTime(playedContent,pausedTime);
}
```

또한 다음과 같은 함수를 통해 콘텐츠를 재생할 때 해당 콘텐츠가 재생 중단을 수행한 콘텐츠 인지를 확인한 후, 중단 콘텐츠일 경우 저장되어 있는 재생 중단 시점을 불러와 그 시점부터 재생할 수 있도록 지원한다.

[표 20] 콘텐츠 재생 함수

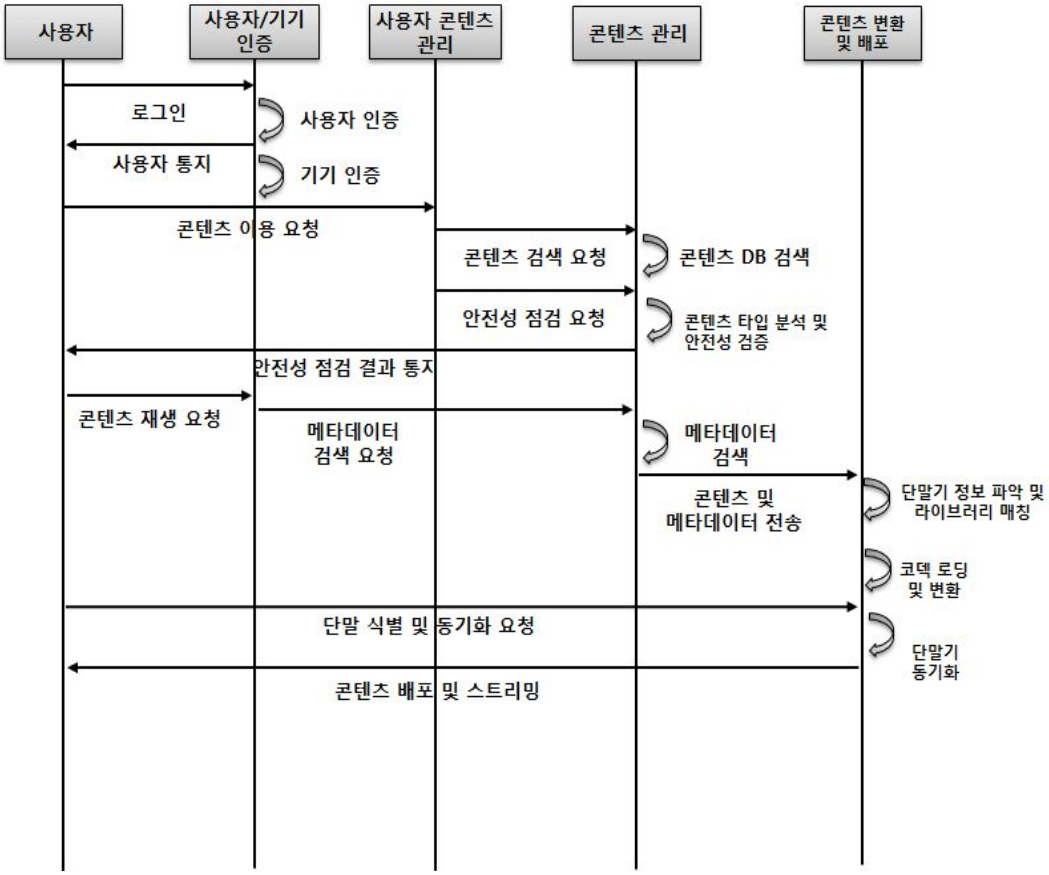
```
function playContent() {
//재생할 콘텐츠 인식 및 주소 지정
var playContent =
      document.getElementsByTagName ('video')[0];
playContent='http://220.69.170.111/educontent/element/math/12-4.mp4'
//재생 중단 콘텐츠 목록 탐색
for(var i=0;i<pausedContent.length;i++)
 { if(playContent == pausedContent[i]){
//재생 중단 시점 로드 및 재생
   playContent.currentTime=
                pausedContent[i].paused Time;
  }
  playContent.play();
}
```

5) 플로우차트

NTCPM을 사용하는 사용자는 일반적으로 크게 세 가지의 과정을 거치게 된다. 첫 번째로 콘텐츠 재생 요청 후 콘텐츠의 안전성 점검, 두 번째로 선택한 콘텐츠의 변환과 전송 및 스트리밍, 세 번째로 콘텐츠의 재생 중단 및 기기 변경으로 나눌 수 있다.

(1)콘텐츠 재생 요청

다음 [그림 12]는 콘텐츠 재생 요청의 플로우차트를 나타낸 것이다.



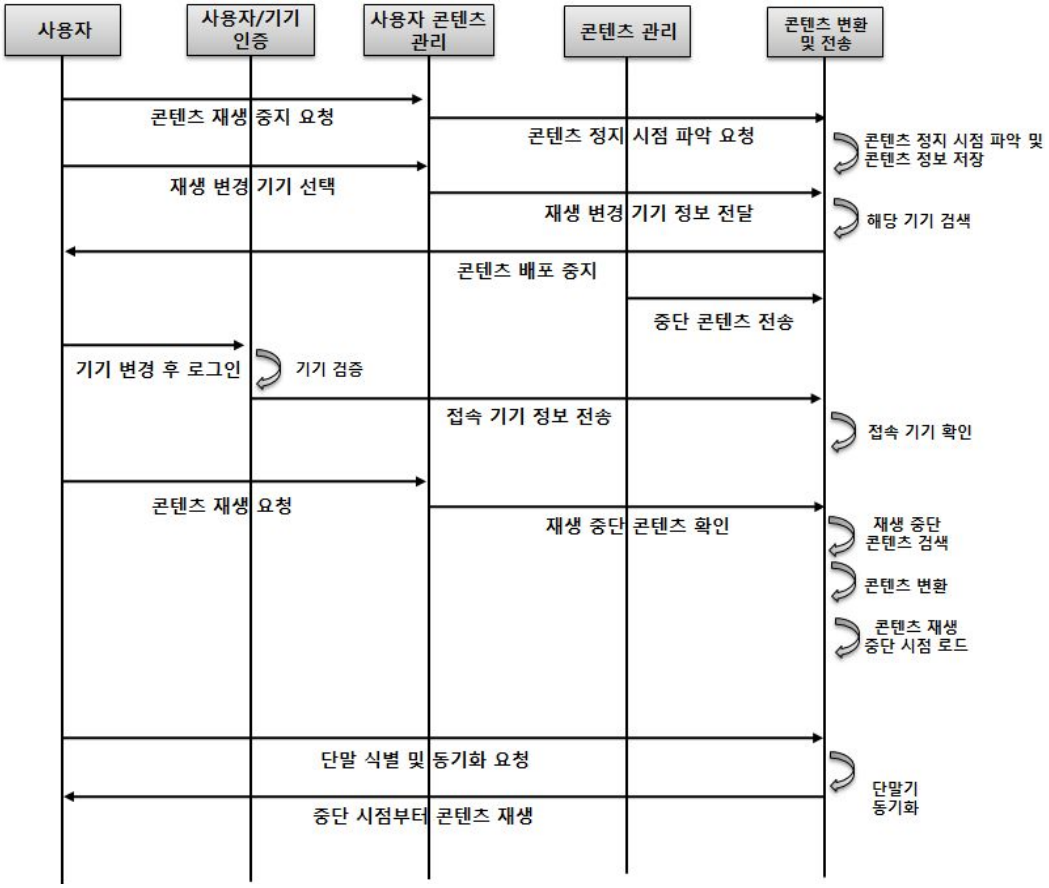
[그림 12] 콘텐츠 재생 요청 플로우차트

콘텐츠의 이용에 있어 사용자는 우선 사용자 인증과 기기 인증을 수행하게 된다. ID와 패스워드를 이용한 사용자 인증을 마친 후 사용자가 접속한 기기 인증을 수행한다. 이 때, 사용자가 접속을 시도하는 기기가 등록되지 않은 기기일 경우, 사용자에게 시스템 이용 시 콘텐츠 재생을 수행할 수 없음을 통지한다.
사용자 및 기기 인증을 마치고 나서 사용자가 콘텐츠의 이용을 요청하면, 콘텐츠 관리에서 해당 콘텐츠를 검색하여 콘텐츠의 안전성 점검을 요청한다. 콘텐츠의 타입을 파악하고 타입에 매치되는 요소에 대해 안전성을 점검하게 되면면 사용자에게 안전성 점검 결과를 통지한다.

콘텐츠의 안전성 검증이 끝나면 사용자는 콘텐츠의 재생을 사용자 콘텐츠 관리에 요청하게 된다. 재생 요청을 받게 되면 콘텐츠 관리에 콘텐츠에 연계 되어 있는 메타데이터의 검색을 요청한 후 메타데이터의 검색이 끝나면 해당 콘텐츠와 메타데이터의 변환을 시도한다. 변환 전에 사용자 기기의 정보를 전송받아 단말 라이브러리에 저장 되어 있는 기기 정보와 비교하여 변환에 사용할 코덱을 로딩한다. 코덱의 로딩이 끝나면 콘텐츠와 메타데이터를 사용자가 요청한 기기에서 사용할 수 있는 형태로 변환한다. 변환이 끝나면 콘텐츠를 전송을 위해 단말을 동기화 시키고 콘텐츠를 스트리밍 형식으로 배포한다.

(2) 재생 중단 및 기기 변경

다음 [그림 13]은 재생 중단 및 기기 변경의 플로우차트를 나타낸 것이다.



[그림 13] 재생 중단 및 기기 변경 플로우차트

사용자가 콘텐츠 재생을 중단하면, 콘텐츠 변환 및 전송에서는 콘텐츠의 정지 시점을 파악하여 이를 저장하고, 중단을 실행한 콘텐츠의 정보 또한 저장한다. 사용자가 흐름에 맞게 재생을 변경할 기기를 선택하면 해당 기기가 시스템에 등록된 기기인지를 파악하고 콘텐츠의 배포를 중지하게 된다. 콘텐츠의 배포가 중지되면, 콘텐츠 관리에서는 중단된 콘텐츠를 새로 변환하기 위해 이를 변환

모듈로 전송하게 된다.

사용자가 기기를 변경한 후 로그인을 시도하면 사용자 인증이 끝나고 난 뒤 기기검증을 하여, 기기에 대한 정보를 콘텐츠 변환 및 전송으로 전달한다. 그 후에 사용자가 콘텐츠의 재생 요청을 수행하면, 사용자가 재생을 중단하였던 콘텐츠를 확인한 후 이를 검색한다. 해당 콘텐츠의 검색이 끝나게 되면 전달받은 기기 정보와 사용자가 변경 전 선택한 기기의 정보를 비교한다. 두 정보가 일치하면 콘텐츠를 해당 기기에 맞는 형태로 변환하고, 사용자가 재생을 중지한 시점을 로드하게 된다. 콘텐츠의 변환 및 전송 준비가 끝나게 되면 사용자 기기의 식별 및 동기화를 수행 한 후에 중단 시점에서부터 콘텐츠를 배포한다.

4. 알고리즘

본 논문에서 제안한 N-Screen 환경 내 신뢰할 수 있는 콘텐츠 이용 방안은 사용자 및 디바이스의 인증을 통한 이용 대상의 제한, 이용하고자 하는 콘텐츠의 타입에 따른 개별적 안전성 검증, 그리고 마지막으로 사용자가 선택한 기기의 특성 및 이용 가능한 콘텐츠의 타입과 종류를 파악하고 매치시켜 알맞은 형태로 변환하여 전송하는 과정으로 구분된다. 다음 [표 21]은 NTCPM의 알고리즘을 나타낸 것이다.

[표 21] NTCPM 알고리즘

Algorithem for NTCPM	
	//사용자 및 디바이스 인증
1:	login_status←Login(id,E(pw));
2:	if login_status is FALSE then
3:	Alert('Login Failure');
4:	else
5:	device_status←Device_Auth(user_device);
6:	if device_status is FALSE then
7:	Alert('your device is not authend');
8:	end if
9:	MovetoMainPage(id,device_status);
	//콘텐츠 선택 및 안전성 인증
10:	content_id←SelectContent();
11:	content←SearchContent(content_id);
12:	SendtoSafetyCheck(content);
13:	switch(content.type){
14:	case TEXT:
15:	content_safety←CheckTextSafety(content);
16:	break;
17:	case AUD:
18:	content_safety←CheckAudSafety(content);
19:	break;
20:	case VID:
21:	content_safety←CheckVidSafety(content);

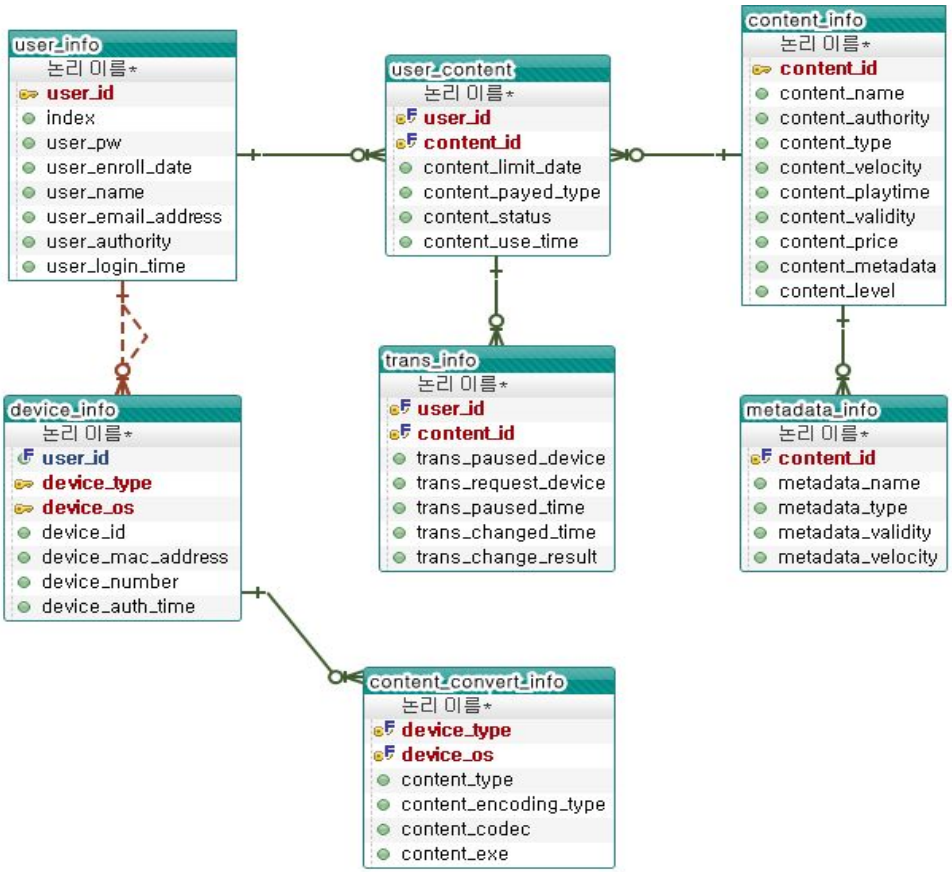
```
22:       break;
23:     case IMG:
24:       content_safety←CheckImgSafety(content);
25:       break;
26:       return content_safety;
27:   }
28:   if content_safety is FALSE then
29:     Alert('This content is not safety);
30:   end if
      //콘텐츠 변환 및 전송
31:   content_metadata←MetadataSearch(content_id);
32:   SenttoConvert(content,content_metadata);
33:   device_type←AnalyzeDeviceType(user_device);
34:   os_type←AnalyzeOSType(user_device);
35:   switch(device_type){
36:     case TV:
37:       tv_type←AnalyzeTVType();
38:       tv_os←AnalyzeTVOS(tv_type);
39:       extension_type←AnalyzeTVExtension(tv_type,tv_os);
40:       SendContentInfo(tv_type,tv_os,extension_type);
41:       break;
42:     case PC:
43:       pc_os←AnalyzePCOS();
44:       extension_type←AnalyzeTVExtension(pc_os);
45:       SendContentInfo(pc_OS,extension_type);
46:       break;
47:     case PAD:
48:       pad_type←AnalyzePadType();
49:       pad_os←AnalyzePadOS(pad_type);
50:       extension_type← AnalyzePadExtension(pad_type,pad_os);
51:       SendContentInfo(pad_type,pad_os,extension_type);
52:       break;
53:     case SmartPhone:
54:       phone_type←AnalyzePhoneType();
55:       phone_os←AnalyzePhoneOS(phone_type);
56:       extension_type← AnalyzePhoneExtension(phone_type,phone_os);
57:       SendContentInfo(phone_type,phone_OS,extension_type);
58:       break;}
```

```
converted_content←ConvertContent(content,content_metadata,content_codec);
if converted_content is valid
sync_device←requestSyncronize(user_device);
 if sync_device = TRUE then
   SendContent(user_device,converted_content);
 end if
end if
//재생 중단 및 기기 변경 추가
change_request←RequestDeviceChange();
 if change_request = TRUE then
   {Alert('request error');}
 end if
changed_device←SelectChangeDevice();
change_device_info←AnalyzeDevice(change_device);
change_content←SaveContent(content);
paused_time←SavePauseTime(changed_content);
converted_content←ConvertContent(change_device_info, content);
 if change_status = TRUE then
   if request_content = changed_content then
     play_time←LoadPausedTime(changed_content);
     sync_device←RequestSyncDevice(change_device);
     SendContent(changed_device, converted_content);
     PlayContent(converted_content, play_time);
   end if
 end if
```

V. 설계 및 구현

1. 데이터베이스 설계

5장에서는 신뢰할 수 있는 안전한 콘텐츠의 제공을 위해 NTCPM에 적용될 DB를 설계한다. 다음 [그림 14]는 NTCPM 내에서 이용되는 정보에 관련된 데이터베이스의 구조 및 관계를 나타낸 것이다.



[그림 14] NTCPM 데이터베이스 구조도

내부 데이터베이스는 6개의 테이블로 구성된다. 등록된 사용자와 관련된 정보를 포함하는 user_info 테이블, 사용자가 서비스를 이용하기 위한 다양한 타입의 디바이스 정보를 포함하는 device_info 테이블, 사용자가 보유하는 콘텐츠의 정보를 포함하는 user_content 테이블, 콘텐츠의 기본 정보를 포함하는 content_info 테이블, 콘텐츠 제공 시 부가정보로서 포함되는 메타데이터의 정보를 포함하는 metadata_info, 콘텐츠 변환 시 활용되는 정보를 포함하는 content_convert_info 테이블, 그리고 콘텐츠의 전송 및 연속 재생에 대한 정보를 포함하는 trans_info 테이블이 존재한다. 다음 [표 22]는 각 테이블에서 활용되는 정보를 나타낸 표이다.

[표 22] 테이블 내 활용 정보 상세

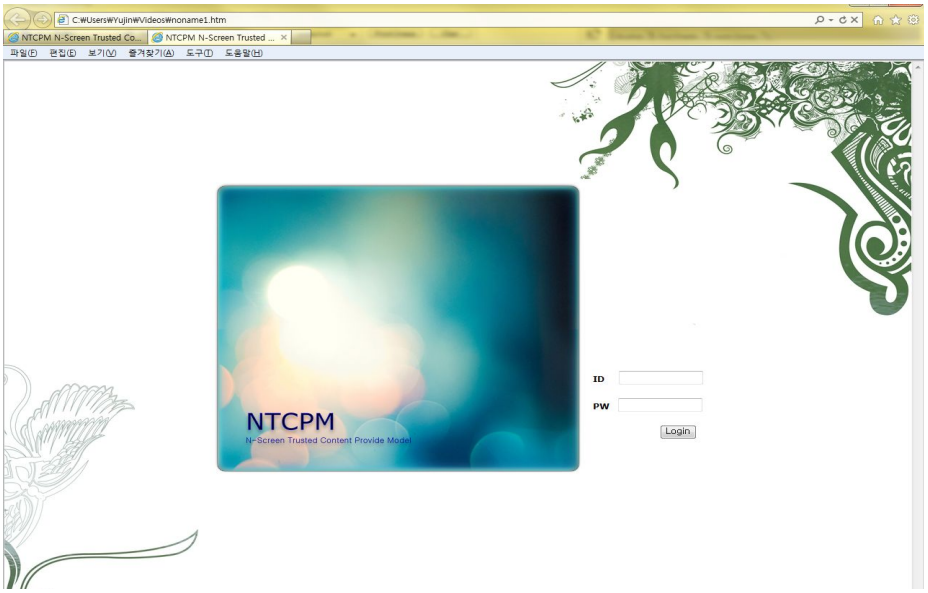
테이블	포함 정보
user_info	사용자 아이디, 패스워드, 이름, 이메일, 등록일자, 권한, 최근 로그인 시간
device_info	디바이스 타입, 탑재 OS, 디바이스 넘버(IMEI), 전화번호, 디바이스 MAC Address, 최근 인증 시간
user_content	사용자 아이디, 콘텐츠 아이디, 콘텐츠 유효 기간, 콘텐츠 결제 여부, 콘텐츠 상태, 최근 콘텐츠 이용 시간
content_info	콘텐츠 아이디, 콘텐츠 이름, 콘텐츠 권한, 콘텐츠 타입, 콘텐츠 용량, 콘텐츠 재생시간, 콘텐츠 유효성, 콘텐츠 가격, 콘텐츠 메타데이터 여부, 콘텐츠 레벨
metadata_info	콘텐츠 아이디, 메타데이터 파일명, 메타데이터 타입(확장자), 메타데이터 유효성, 메타데이터 용량
content_convert_info	디바이스 타입, 탑재 OS, 콘텐츠 타입, 콘텐츠 인코딩타입, 변환 코덱, 콘텐츠 확장자
trans_info	사용자 아이디, 콘텐츠 아이디, 사용자 중단 기기 정보, 사용자 재생 개시 기기 정보, 콘텐츠 중단 시간, 기기 변경 수행 시간, 기기 변경 결과

2. 프로토타이핑

NTCPM은 Windows 7 운영체제에서 구현되었으며 웹 환경은 Apache Tomcat 7.0 버전을 지원한다. 구현 언어로는 HTML5, CSS3, Javascript 그리고 JSP를 사용하였으며 DBMS는 MySQL 5.5 버전을 사용하였다. 구현 툴은 Visual Studio 2012 express for web, 그리고 Eclipse를 이용하였다.

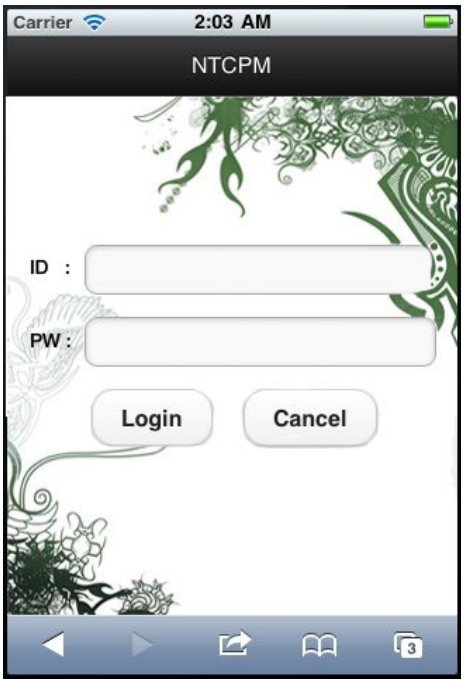
스마트폰 및 스마트 패드 환경에서의 상호호환성을 지원하기 위해 HTML5 언어 기반으로 구현하였기 때문에 iOS, Android, Windows Phone등의 모바일 OS와 Explorer, Safari, Chrome 등의 대부분의 웹 브라우저에서 본 모델을 조회할 수 있다. 사용자는 본 인터페이스를 통해 자신이 보유하고 있는 콘텐츠를 확인하고 재생을 요청하여 안전성을 검증한 후 콘텐츠를 재생할 수 있다. 또한 콘텐츠의 재생 중단 및 기기의 변경 또한 가능하다.

1) 메인 화면



[그림 15] NTCPM 메인 화면

[그림 15]는 NTCPM을 PC에서 접속했을 때 보여지는 메인 화면이다. 아이디와 패스워드를 입력하여 사용자의 로그인을 시도할 수 있다. [그림 16]은 모바일 화면에서의 NTCPM의 메인 화면이다. 모바일에서 접근할 경우 사용자 인증 후 이루어지는 기기 인증 과정에서, 사용자의 시스템 상에 등록되지 않은 기기로 접속했을 경우에는 [그림 17]과 같이 사용자에게 통지하고, 시스템의 일부를 이용할 수 없음을 고지한다.

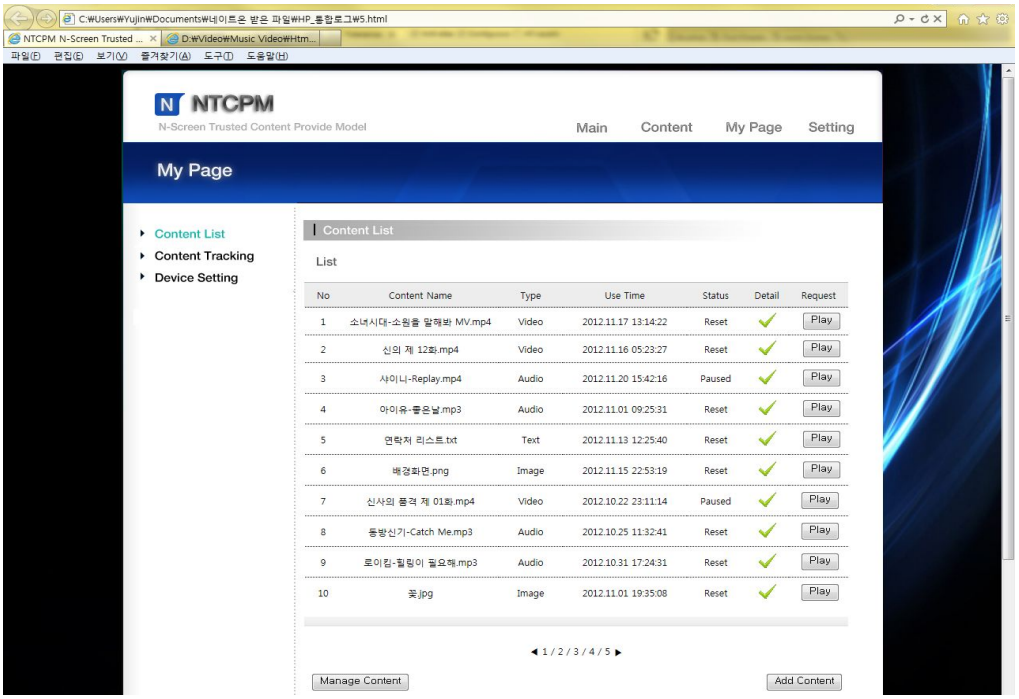


[그림 16] 모바일 로그인 화면

[그림 17] 사용자 경고창

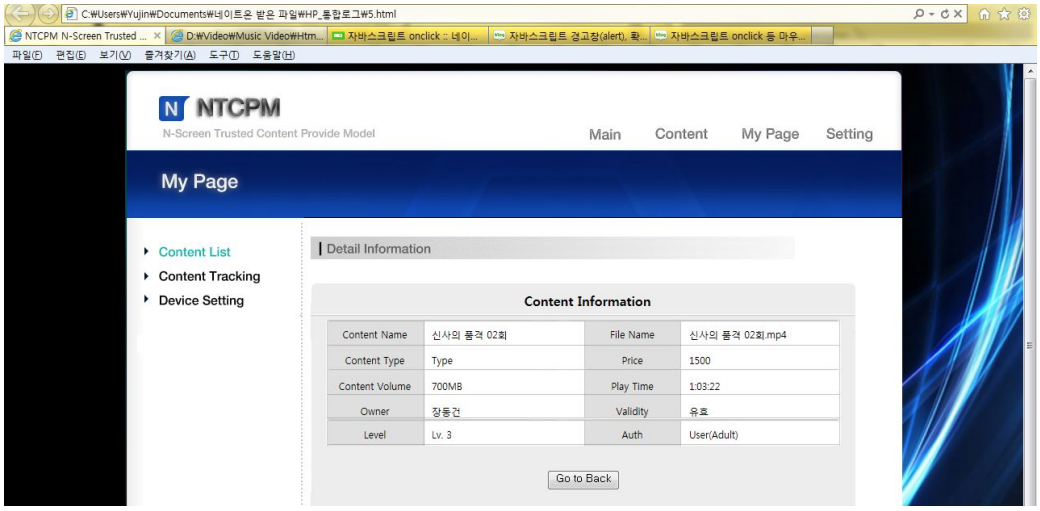
2) 사용자 콘텐츠 관리 화면

[그림 18]은 사용자 콘텐츠 화면을 나타낸 그림이다. 사용자 콘텐츠 관리에서는 사용자가 현재 보유하고 있는 콘텐츠의 리스트를 일괄적으로 표지한다. 사용자는 본 화면에서 보유하고 있는 콘텐츠 및 사용자 소유 디바이스에 대한 설정을 수행할 수 있다.



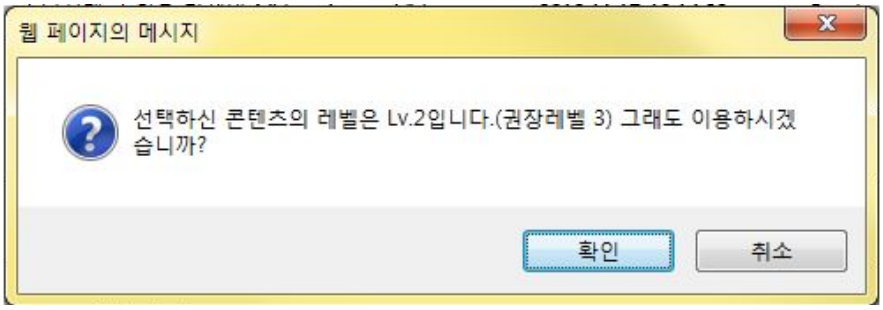
[그림 18] NTCPM 사용자 콘텐츠 관리 화면

사용자는 사용자 콘텐츠 관리 화면을 통하여 보유하고 있는 콘텐츠의 상세 정보를 조회할 수 있다. 콘텐츠 상세 정보 조회 화면은 다음 [그림 19]와 같다.



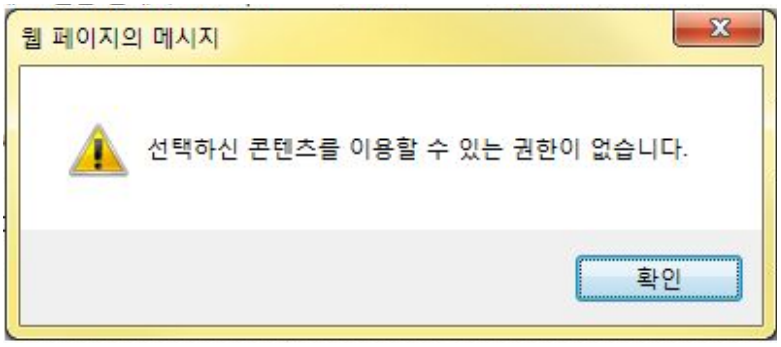
[그림 19] NTCPM 콘텐츠 정보 확인 화면

사용자는 콘텐츠를 이용하고자 할 때 콘텐츠 관리 화면에 표지되어 있는 'Play'버튼을 통해 콘텐츠 이용을 요청하게 된다. 콘텐츠 이용을 요청할 때 콘텐츠에 대한 권한 및 안전성 검사가 이루어지게 된다. 콘텐츠의 권한 및 안전성 검사에 대한 사용자 통지는 다음과 같은 화면으로 표지된다.



[그림 20] 콘텐츠 레벨 알림 팝업

[그림 20]과 같은 팝업 알림을 통해 사용자에게 선택한 콘텐츠의 레벨 및 이용 권장 콘텐츠 레벨을 고지한 후 권장 안전성 레벨이 낮은 콘텐츠 일지라도 사용자가 이용할 수 있는 선택권을 주도록 한다.

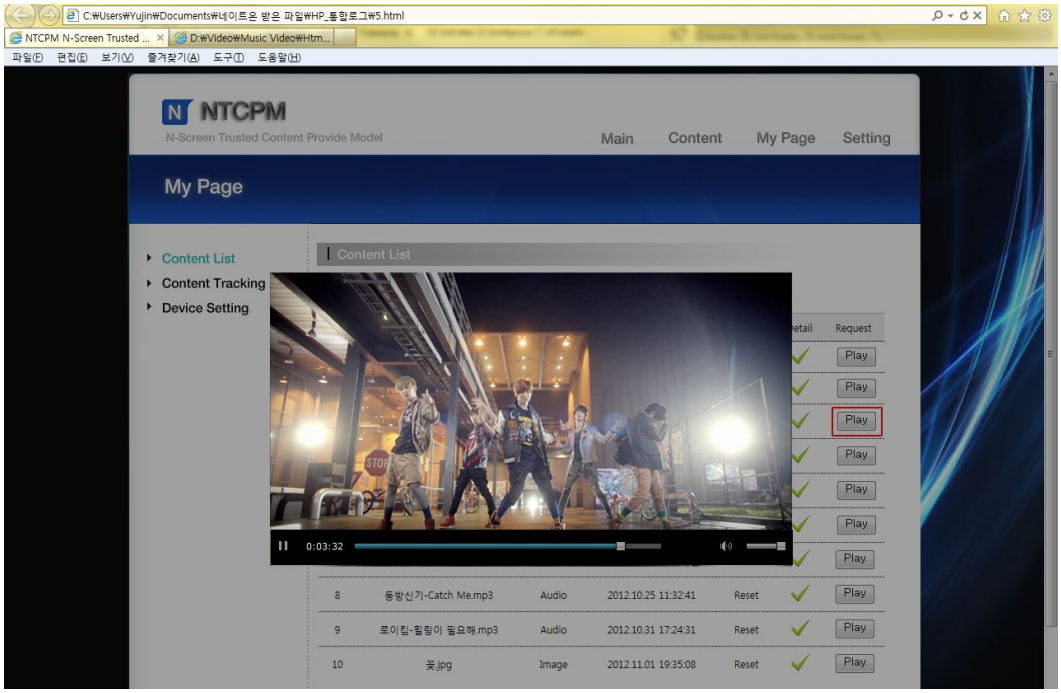


[그림 21] 콘텐츠 이용 권한 알림 팝업

또한 [그림 21]과 같은 팝업 알림을 통해 만약 권한이 부족한 사용자가 권한 밖의 콘텐츠 이용을 요청할 시에는 요청을 거부하고 권한에 대한 사항을 고지한다.

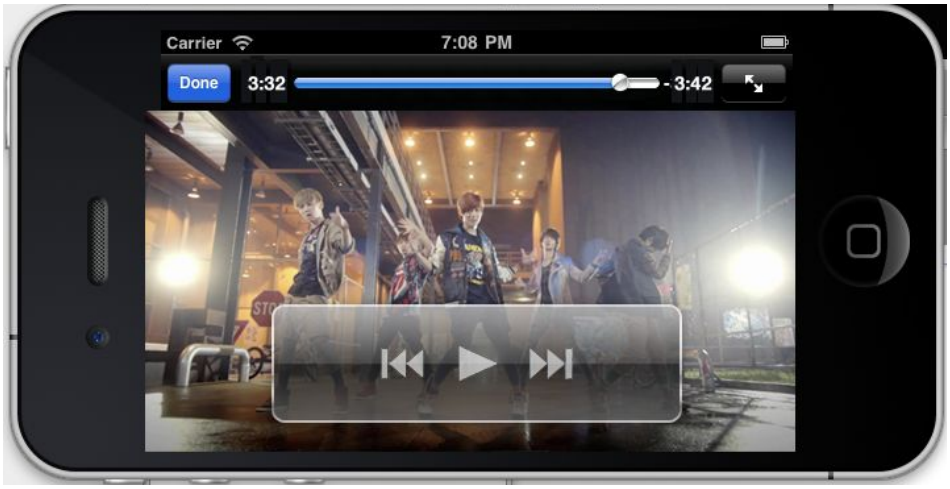
3) 콘텐츠 이용

사용자의 권한 및 콘텐츠의 레벨이 안전하다고 판정된 경우에는 해당 플레이어를 통해 콘텐츠를 재생할 수 있도록 한다. 다음 [그림 22]는 웹 화면에서 요청 콘텐츠를 재생하는 화면이다.



[그림 22] 웹 화면에서의 콘텐츠 재생 화면

웹과 같은 경우 HTML5 언어 내부에 포함되어 있는 <video> 태그를 통해 웹 페이지 상에서 특별한 플러그인을 사용하지 않아도 콘텐츠를 재생할 수 있도록 한다. 또한 모바일에서는 모바일 OS가 지원하는 기본 플레이어를 통해 콘텐츠를 재생할 수 있도록 한다. 다음 [그림 23]은 모바일 화면(iOS)에서 재생되는 콘텐츠를 나타낸 화면이다.



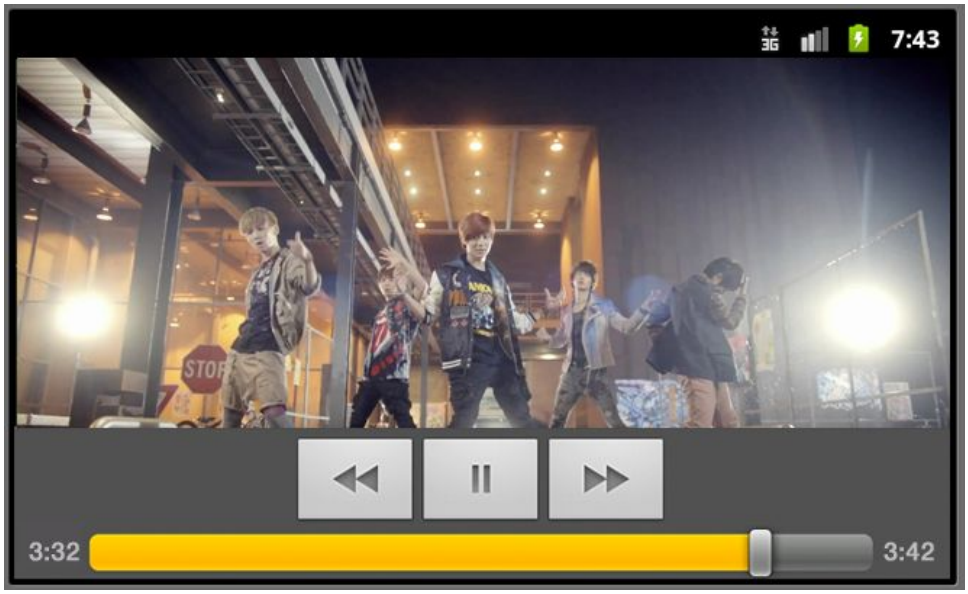
[그림 23] iOS에서의 콘텐츠 재생 화면

4) 재생 중단 및 기기 변경

사용자는 콘텐츠를 재생하던 기기에서 시스템 상에 등록 되어 있는 다른 기기로 재생 변경을 요청할 수 있다. 다음 [그림 24]는 iOS 환경에서 콘텐츠 재생 중, 일시정지 화면을 눌렀을 때 나타나는 기기 선택 화면을 나타낸 것이다.

[그림 24] iOS에서의 재생 중단 화면

본 화면에 뜬 팝업창을 통해, 시스템에 등록되어 있는 사용자의 기기들을 로드하여 사용자가 선택하게 되면, NTCPM으로 해당 기기의 선택 여부 및 재생 중단된 콘텐츠에 대한 정보가 저장되고 이용하고 있던 기기에서는 콘텐츠 이용이 중지된다. 다음 [그림 25]는 새로운 기기 환경(Android)에서 사용자가 로그인을 한 후 콘텐츠의 연속재생을 요청하여 중단시점부터 콘텐츠가 재생되는 화면이다.



[그림 25] 기기 변경 후 재생 화면(Android)

사용자가 기기를 변경하고 난 후 변경 기기의 정보 및 연속재생 요청 콘텐츠의 정보를 불러오고 나면 HTML5 언어의 <video>태그의 속성을 이용하여 중단 시점을 로드하고, 해당 시점부터 콘텐츠를 재생할 수 있도록 한다.

Ⅵ. 결론 및 향후 연구

모바일 OS를 탑재한 다양한 형태의 스마트 디바이스들의 수요가 증가함에 따라 새로운 형태의 서비스 및 대용량 멀티미디어 콘텐츠들의 수요 또한 폭증하고 있다. 그러나 다양한 기기를 연동하여 사용하게 되는 서비스가 등장하게 되면서 이에 따라 스마트 디바이스를 통한 콘텐츠 이용에서의 안전성의 부족, 개인정보에 대한 새로운 위협이 야기되었다.

이와 같은 문제점을 해결하고자 본 논문에서는 N-Screen 환경 내에서 다양한 형태의 콘텐츠 이용 중 발생할 수 있는 문제점을 도출하고 이를 보완하기 위해 N-Screen 환경 내 신뢰할 수 있는 콘텐츠 이용 방안을 설계 및 구현하였다.

각종 스마트 디바이스들이 증가하고 있는 추세에 따라 앞으로 N-Screen 환경 내에서의 콘텐츠 이용률이 폭발적으로 증가할 것으로 예측되는 가운데 NTCPM의 설계 및 구현을 통해 기기 제조사 및 소프트웨어 벤더의 정책에 종속되어 이용할 수밖에 없는 현재 서비스 경향과는 달리, 사용자가 기기 및 시스템과 같은 환경의 제약 없이, 자유롭게 콘텐츠를 이용할 수 있도록 하는 방안을 제시함으로써 개방되고 확장된 환경에서의 콘텐츠 이용을 도모하였다. 그리고 상대적으로 안전성에 취약했던 N-Screen 환경 내에서의 콘텐츠 이용에 있어서의 개인정보의 보호 및 권한별 등급 분류에 따른 안전한 콘텐츠 이용을 제공함으로써 새로운 환경에서 발생할 수 있는 개인정보 및 등급별 콘텐츠 이용에 대한 문제점 또한 해결할 수 있을 것으로 사료된다.

향후에는 본 논문에서 제안한 시스템에 개인정보보호법을 기준으로 한 정책을 적용하여 법적으로 개인정보를 보호할 수 있는 방안을 연구할 예정이다. 또한 HTML5 언어를 이용한 멀티미디어 콘텐츠의 효율적인 관리 및 스트리밍의 제어 방안에 관하여 연구할 예정이다.

참고 문헌

[1] 윤용익 외 1, “N-Screen 표준화 고려사항 및 전략의 등장”, 정보과학회논문지 제 29권 7호, 한국정보과학회, 2011

[2] 김화숙 외 2, “N-Screen 서비스 현황 및 연구 개발 이슈“, 정보과학회논문지 제29권 7호, 한국정보과학회, 2011

[3] Peter Mell, Timothy Grance, “the NIST Definition of Cloud Computing (Draft)”, NIST, 2011

[4] Mark D.Ryan, “Cloud Computing Privacy Concerns on Our Doorstep”, Communications of the ACM, 2011

[5] DLNA, “DLNA Interoperability Guidelines version 1.5”, DLNA, 2006.

[6] 안병현 외 1, “HTML5 표준화 현황과 활용 사례”, 정보과학회논문지 제30권 5호, 한국정보과학회, 2012

[7] 이은민, “HTML5가 웹 환경에 미치는 영향”, 정보과학회논문지 제29권 6호, 한국정보과학회, 2011

[8] P.Mika, M.Greaves, “Semantic Web and Web 2.0”, joutnal of web semantics, 2012

[9] 양형규 외 1, “UCC 저작권 보호를 위한 DRM 시스템”, 한국컴퓨터정보학회지 제15권 2호, 한국컴퓨터정보학회, 2010

[10] Q.Liu, R Safavi-Naini, and N.P.Sheppard, “Digital rights management for content distribution”, proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, Vol.21. 2003

[11] 임영권 외 2, “이동 멀티미디어 방송용 멀티미디어 압축 방식”, 한국방송공학회지 제8권 1호, 한국방송공학회, 2003

[12] 홍승필, “개인정보보호 개론, 사례 연구 및 기술 중심으로”, 한티미디어,

2009
[13] 한국인터넷진흥원, “정보통신 서비스 제공자를 위한 개인정보보호 법령 해설서”, 2012
[14] 개인정보보호위원회, “개인정보보호 연차보고서”, 2012
[15] OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flowers of Personal Data”, 2001
[16] 김진형 외 1, “정보유출방지와 프라이버시 침해에 대한 고찰”, 정보보호학회논문지 제21권 5호, 한국정보보호학회, 2011
[17] 문신용 외 1, “공공기관의 개인정보 침해사례 분석의 함의 및 과제”, 한국행정연구 제13권 4호, 한국행정연구원, 2005
[18] 남기효 외 4, “개인정보보호기술의 최신 동향과 향후 전망”, 정보보호학회논문지 제18권 6호, 한국정보보호학회, 2008
[19] 강미란 외 3, “다중 기기에서 이어 보기를 위한 동기화 기법”, 한국콘텐츠학회논문지 제 11권 12호, 한국콘텐츠학회, 2011
[20] 최헌회 외 1, “HTML5 기반 HTTP 스트리밍 환경에서의 서비스 이동성 연구”, 한국멀티미디어학회논문지 제 14권 7호, 한국멀티미디어학회, 2011

Abstract

Designing and Implementing of N-Screen Trusted Content Provide Model

Yu-jin Shin
Dept. of Computer Science
The Graduate School
Sungshin Women's University

In this paper, we propose a model of trusted multimedia content provision which assure not only safety of content but also flexibility of content use. N-Screen environment is a new service paradigm which appeared by the spread various smart device, represented by smartphone. Because one user can have many type of device, the OSMU(One Source Multi Use) issues by the content which is user has. But the policy of device and mobile OS vender is different, OSMU is hard to established to user who has various type of device and mobile OS. And, new smart device environment are made rapidly, so illegal and insecure content

spread. So, demand of safe content use in smart device environment are increased.

In order to solve this problem, in this paper, we design and implement the NTCPM(N-Screen Trusted Content Provide Model). In this paper, we studied the way to use same service in various type of OS and device environment. Also we studied method to provide safe content in N-Screen environment.

Through the model which is propose in thie paper, we do not limited by environment of device and OS, and can use many type of multimedia content flexibly. And we can expect the effect of provision secure content to multi device user by the various type of content verification.