Journal of The Korea Society of Computer and Information
Vol. 21 No. 12, pp. 59-72, December 2016
www.ksci.re.kr
https://doi.org/10.9708/jksci.2016.21.12.059

An Efficient Application of eBSS DRM Method to eBook Contents based on ePub 3.0 for Smart Device

Eung Sup Jun*

Abstract

DRM(Digital Rights Management) is essential for the copy right protection of eBooks based on ePub 3.0 by IDPF. In this paper, we developed eBSS(eBook Service System) as ePub 3.0 builder and viewer system with DRM and proposed an efficient DRM method which improves the performance of contents generation, security and distribution system. The efficient application of DRM method to the eBook contents based on ePub 3.0 for smart phone is practically useful for eBook service system. It is very useful for the suggested eBSS with DRM method and strategy to apply easily and practically to the encryption and decryption of the eBook contents. Also, it is very efficient to generate the ePub 3.0 contents and to apply DRM method to it especially, by using practically this suggested ePub 3.0 builder system from the view point of the eBook content generation and its viewer such as eBook reader for user and eBook providers.

▸ Keyword : DRM, ePUb 3.0, eBook, Smart Device

I. Introduction

디지털 콘텐츠의 급속한 보급과 더불어 스마트 단말기를 이용한 전자책 콘텐츠의 사용이 보편화 되면서, ePub기반의 콘텐츠 개발과 보급을 효율적으로 관리하고 운용하는 체계가 필요하다[1]. DRM은 콘텐츠의 지적 재산권이 디지털방식에 의해서 안전하게 보호 및 유지되도록 하여 콘텐츠가 제작에서부터 소비에 이르기 까지 모든 유통단계에서 거래와 분배 규칙, 사용규칙 등이 적법하게 이루어지도록 하는 기술이다. 이미 국내외적으로 전자책은 IDPF(International Digital Publishing Forum)에서 전자책 기술규격의 표준으로 마련한 ePub(Electronic Publication) 표준을 기반으로 전자책을 제작하고 유통하는 체계를 갖추고 있다[2,3,4]. 여기에 발 맞추어 전자책의 불법복제 방지 및 저작권 보호를 위한 다양한 DRM의 적용과 솔루션이 각각의 상이한 기술규격을 기반으로 적용되고 있어 전자책의 공급 및 유통에 있어서 각 개발업체 간에 상호 운용성이 보장되지 않고 있다. 이처럼 DRM기술의 상호 운영성 부재는 DRM기술에 종속적인 전자책 공급체계와 전자책 이용상의 불편성을 야기하는 등 여러 문제점이 있다[5]. 본 연구에서는 이러한 문제점을 해결하기 위한 방안으로 스마트기기에서 사용자들이 쉽게 전자책 콘텐츠를 구매하여 구독할 수 있는 ePub 3.0 기반의 콘텐츠 제작과 이의 불법 복제를 방지하고 저작권을 보호할 수 있는 최적의 DRM 적용 기법과 응용사례를 제시한다. 최근에 스마트기기를 중심으로 사용되는 전자책의 제작과 이들 콘텐츠의 보급 확대가 점증하고 있고, 이를 위해 사용자에게 즉시로 제공할 수 있는 시스템과 다양한 솔루션이 제공되고 있다. 그러므로 스마트기기용 콘텐츠제공에서 보다 효율적이고 신속한 양질의 콘텐츠를 배포시키고 안전한 콘텐츠를 보호 하는 기술인 DRM의 최적 적용방법은 디지털 콘텐츠의 제작과 유통에 있어서 매우 큰 비중을 차지하고 있다. 그러나 DRM기술의 상호 운용성 부재는 DRM기술에 종속적인 전자책의 공급체계와 전자책 사용의 불편성 등 여러 문제점이 제기되고 있다. 본 제안 시스템에서는 이러한 해당 전자책의 본문이 휴대용 스마트 기기의 리

• First Author: Eung Sup Jun, Corresponding Author: Eung Sup Jun
*Eung Sup Jun(esjun@induk.ac.kr), Dept. of Computer Software, Induk University
• Received: 2016. 11. 26, Revised: 2016. 12. 08, Accepted: 2016. 12. 23.
• The research was supported by an academic research fund and grant of Induk University.

더기인 뷰어에서 즉시 펼쳐지고, 전자책 전문을 '일부 보기', '설정한 분량 보기', '전문 보기' 등 DRM 사용 권한에 따라 구분하여 서비스 할 수 있는 eBSS(eBook Service System)에서 최적화된 DRM적용 방법을 제시한다. 또한, 새로운 전자책 콘텐츠를 호환성 있는 암복호화로 유통시켜 사용자가 스마트기기를 사용하여 원하는 eBook콘텐츠를 구매하고 앱으로 제공된 스마트폰 뷰어를 통해 손쉽게 구독할 수 있게 한다. 본 논문의 구성은 II장에서 국내외의 ePub표준화 현황과 이에 관련된 DRM 적용의 연구동향 및 국내 시장에서의 문제점을 살펴보고, III장에서 최적의 전자책 제작을 위한 효율적인 DRM 적용기법을 제시하며, IV장에서는 실제 적용될 eBSS시스템의 주요 처리절차와 기법을 최적화한 UML분석과 설계를 제시하고 V장에서 프로토타입을 구축하여 최적화된 DRM 기법을 적용하여 국내의 5개의 서적을 ePub빌더로 제작하고 전자책의 암복호화 하는 내용을 화면중심으로 보여준다. 마지막 VI장에서는 본 제안 시스템을 활용하여 실제 전자책의 제작과 암복호화를 적용한 후에 실제 사용자를 중심으로 본 시스템의 사용자 만족도를 설문조사하여 그 효과를 측정 및 분석하고 마지막으로 결론과 향후 연구과제를 제시한다.

II. Related Works

1. Literature Reviews

1.1 ePub 표준화 현황

전자책의 표준기술 규격으로 IDPF에서는 2007년 ePub 표준을 제정하였으며, 이후 2010년 ePub 2.0, 2011년 ePub 3.0 표준을 발표하였다[6,7]. IDPF의 ePub 표준은 PDF가 주류를 이루고 있는 전자책 산업에 새로운 기술 표준을 제시하고 있다. IDPF의 기술 표준화에 따라 2009년 이후에는 스마트 기기를 포함한 다양한 모바일 기기들이 ePub 포맷을 지원하는 전자책 viewer 소프트웨어를 탑재하여 출시하고 있고, 국내외 전자책 서비스 제공자들도 대부분 ePub 표준을 필수 지원 포맷으로 채택하고 있다. ePub은 국제적으로 전자책 산업의 표준으로 되고 있으나[8,9], ePub 표준의 OCF(Open Container Format) 기술명세서에서 권고하고 있는 암호화 및 전자서명의 보안 가이드라인은 W3C의 암호화 및 전자서명을 표준으로 명시하고 있을 뿐 구체적인 알고리즘이나 적용 방법 등에 대한 설명이 없는 상태이다. W3C에서 권고하고 있는 XMLEncription과 Signature 표준은 다양한 적용방법에 따라 전자책 제공 업체마다 표준의 이해 및 구현방식이 다르고, ePub DRM의 개발방식들 간에 상호호환이 될 수 있는 효율적인 지원체계가 없는 실정이다[5].

1.2 국내외의 동향

다음 Table 1.에서 보는 바와 같이, 국내에서 전자책에 대한 관심과 활성화로 교보문고 및 인터파크 등이 각자의 전자책 전용 단말기나 고유의 SW기술을 사용하여 전자책 시장의 선점과 확장을 하고 있다.

Table 1. eBook Service Suppliers in Domestic Market

Company	Pro-duct	File Form-at	DRM	Provider	Distribution
Amazone	eBook	AZW	Closed Technology	Amazone	Internet Bookstore B2C Special Purpose Terminal App.
Kyobo-book	eBook	Private PDF	DRM Technology of eBook Company & Terminal Manufacturers	Fasoo Unidocs	Library B2B / B2C Special Purpose Terminal, Smart App., PMP
Interpark	eBook	Private		Markany	Library B2B / B2C Special Purpose Terminal, Smart App., PMP, PC
Korea Electronic Publishing Hub	eBook	ePub		Incube	Library B2B / B2C Smart App., PC
Bookcube	eBook	BCB		Dasangng	Library B2B / B2C Smart App., PC
Ridibooks	eBook	ePub		Ridibooks	Internet B2C Smart App.

국외에서는 Table 2.에서 보는 바와 같이, 애플, 구글 등 주요 IT업체를 중심으로 전자책의 제작 및 유통의 전 과정에 걸쳐서 일련의 라인업화 된 서비스 플랫폼을 갖추고 전자책 서비스를 제공하고 있다. 또한 이들은 전자책 시장의 활성화를 위해서 IDPF에서 표준으로 제정하고 있는 ePub표준을 지원하고 있다[4].

Table 2. eBook Service Suppliers in Overseas Markets

Company	Product	File Format	DRM	Terminal	Service
Apple	eBook	ePub	FairPlay	iOS Device	iBooks, iBook Store
Google	eBook	ePub	Adobe	-	Google Editions
Sony	eBook	ePub	Adobe	Sony Reader	Sony eBook Store
Borders	eBook	ePub	Adobe	Kobo, Smart phone, Libre eBook Reader	Borders eBook Store
Barnes & Noble	eBook	ePub	Adobe	Nook	eBook Store Pubit

2. ePbu DRM Interoperability Technology Specification

2.1 국내 전자책 DRM 연구 동향

현재 DRM관련된 국내의 연구 동향은 다음 Table 3.에서 보는 바와 같이, 크게 모바일 환경에서 최적으로 적용 가능한 방법과 ePub기반의 표준화 적용기법 그리고 효율적인 DRM 분배키 관리방식으로 나눌 수 있다.

Table 3. Domestic Research Trends related in DRM

Study	Researcher	Year	Title of Research
Mobile Base	Jun,Chang	2014	An eBook Service System based on VOD Broadcasting Contents of Smart TV
	Kim,Kang, Youn	2012	A Proposal on Secure Partial Encryption for Mobile Digital Rights Management
	Jun,Chang, Oh, Choi	2014	A Framework for Hybrid eBook Service System based on Mobile Smart Device and Smart TV Broadcasting Contents
	Yang,Kim, Seo,Oh	2009	Analysis and Design system of contents partial encryption for Mobile DRM environment
	Cho	2010	Design and implementation of packaging mechanism for protection of DRM contents in Mobile environment
ePub Standard Base	Kim,Ahn, Lee	2014	Consideration of necessity to standardize the e-book DRM
	Yi, Choi, Chin,Joe	2012	DRM applying method for ebook service based on EPUB standard
	Kang, Kim, Yoon, Cho	2011	A Study of ePub-based Standard Framework Supporting Mutual Comparability of eBook DRM
	Kim,Kim, Kim, Cho	2012	A Study of Partial Preview Control Method of ePub-based eBook DRM
DRM Key Manage-ment Base	Sung	2004	Design of CEK Distributed Management System for Secure DRM Key Management
	Song	2009	Anonymous DRM System for Super-Distribution
	Choo,Lee, Jun	2005	Design Secure Key of Decryption Distribution System for DRM System

상기에서 보는 바와 같이 최근에 DRM 관련 연구는 과거 DRM 키 분배 및 관리에 관련된 연구에서 현재는 스마트폰을 중심으로 한 모바일 디바이스 상에서 최적의 DRM적용과 운용기법에 관련된 연구가 이루어지고 있다. 여기에 국내의 전자책 시장의 활성화를 위한 DRM 표준의 공통적 적용으로 사용자의 편리한 전자책 이용성을 높이기 위한 ePub기반의 표준화 적용기법 및 적용사례가 주를 이루고 있다.

2.2 국내 전자책 DRM 기술 현황

상기에서 본 바와 같이 국내에서 연구되고 있는 DRM관련 적용기술과 산업통상 자원부 국가기술 표준원의 ePub DRM 상호운용의 기술명세에 관한 공청회 발표와 관련 국내 연구들의 분석을 통해 국내에서 DRM활성화에 문제가 되는 점들을 다음과 같이 열거할 수 있다[5].

1) 비호환 DRM 기술의 적용

전자책은 디지털 콘텐츠의 특성상 기술적 보호조치가 없는 상태에서 콘텐츠가 유통될 경우 소비자들의 불법 복제를 통해 무차별 재배포가 될 수 있기 때문에 콘텐츠 제공자들은 전자책의 불법복제를 방지하기 위한 수단으로 DRM을 통한 기술적 보호조치를 한다. 그러나 현재 전자책의 저작권 보호를 위해 사용되는 DRM은 산업적으로 통일된 표준화가 되어있지 않아서 전자책 사업자들은 각기 고유한 DRM기술을 적용할 수 밖에 없다. IDPF에서는 이러한 ePub 표준안을 마련하면서 암호화, 전자서명, 권리정보 등에 대한 가이드 라인을 제시했다. 그러나 보안 가이드라인에서 권장하고 있는 W3C XML Encryption과 Signature의 적용방법이 다양하고, DRM솔루션 제공 업체들의 표준에 대한 이해 방식에 차이가 있어 구현된 방식들이 상호운용 될 수 있을 정도의 호환성을 지원하지 못하고 있다.

2) 콘텐츠 사용자의 불편 증가

콘텐츠 제공자들과 서비스 제공자들이 서로 다른 DRM 기술을 사용함에 따라 이들 기술을 적용하고 있는 뷰어 즉 리더기가 동일한 형태로 사용자에게 제공되기가 어렵다. 따라서 사용자들은 ePub표준이 적용된 전자책임에도 불구하고 다른 종류의 DRM 기술이 적용된 두 곳 이상의 서비스 업체로부터 전자책을 구매했을 경우 복수개의 전자책 열람 소프트웨어를 각각 설치하고 이용해야 하는 불편함이 있다. 이로 인해 소비자들은 자신이 구매한 전자책 리스트를 전체적으로 관리하기 어려울 뿐만이 아니라 자신이 선호하는 전자책 뷰어를 사용할 수 없게 되는 경우가 생긴다.

3) 콘텐츠 공급체계의 비효율성 증가

전자책 서비스 사업자들은 복수개의 콘텐츠 제공자들로부터 콘텐츠를 공급받아 판매해야 하는 경우가 있다. 특히, 전자책 공급망이 다양해 지고 있는 현실에서 서비스 사업자들은 복수의 공급업자들이 적용하는 각기 다른 DRM 기술이 적용된 복수의 뷰어들을 소비자의 기기에 설치하거나 자신들이 사용하고 있는 뷰어에 복수의 DRM 기술을 임베디드해야 되는 문제가 생긴다. 이것으로 인해 소비자의 기기에 설치되는 소프트웨어의 개발비용을 증가시킬 뿐만이 아니라 유지보수 측면에서 복잡성을 증가 시키고 있다.

III. DRM Technology for eBooks

현재 국내에서 제기 되고 있는 DRM 표준과 관련한 여러 문제점과 이를 해결하기 위한 효율적인 DRM적용 방식을 고려한 모바일 기반의 eBSS를 구축하기 위해서 다음과 같은 문제점을

살펴본다. 본 논문에서는 생산된 콘텐츠를 다양한 리더기상에서 관련 eBook의 내용을 뷰어로 손쉽게 볼 수 있는 ePub 빌더 시스템의 뷰어기에 적용될 DRM의 효율적 적용을 위해 국내 공통 표준으로 향후 적용될 기준을 국가 기술표준원[5]의 표준안을 중심으로 다음과 같이 정의하고 이를 본 제안 시스템에서 적용한다.

1. Non-Interoperability of DRM Technology

현행 전자책 DRM 기술을 활용한 서비스 사업자는 고유의 DRM 기술로 암호화 하고 사용에 있어 허락을 하는 체계로 되어있다. 일반적으로 판매되는 전자책은 특정 DRM 기술을 이용하여 암호화 되고, 전자책 구매 이용자에게는 특정 DRM기술에 기반한 DRM서버를 통해서 라이선스가 발급되며, 이것들은 특정 DRM클라이언트가 포함된 뷰어에서만 작동한다. 또한 DRM기술로 암호화되어 있는 전자책의 라이선스를 얻기 위해서는 해당 서비스 사업자의 DRM서버에 접속해야 한다. 이러한 시스템구조에서는 DRM서버와 DRM클라이언트 그리고 전자책 뷰어가 하나의 라인업으로 형성하고 있어서, 다른 DRM기술과의 호환성이 허용되지 않는 근본적인 문제점이 있다.

일반적인 디지털 콘텐츠와 달리 전자책의 경우에는 IDPF에서 권장하고 있는 기본 ePub포맷과 W3C 기반의 암호화 및 전자서명 기술에 대한 표준이 이미 수립되어 있고, 대부분의 전자책 서비스 업체들이 ePub기술을 적용하고 있기 때문에 해결이 비교적 용이하다. 즉, IDPF에서 권장하고 있는 보호기술 가이드중 이기종 DRM 간의 완전한 호환을 위해서 명확하게 정의되지 않은 부분을 구체적이고 명확한 표준으로 정의하고, 서비스 사업자들이 이에 대한 표준을 준수한다면 상기에서 언급된 문제점들을 극복할 수 있다.

2. Non-Interoperability Causes of DRM Technology

전자책 DRM기술들 간의 호환성이 보장되지 않는 이유는 서로 다른 전자책 포맷을 사용하여 근본적으로 호환이 불가능한 상황과 동일한 ePub 표준을 사용하고 있음에도 불구하고 라이선스 발급을 위한 프로토콜 표준의 부재 등과 같이 다양한 형태로 나타난다.

2.1 비표준 전자책 포맷 및 보호기술 사용

전자책 서비스 사업자들이 사용하고 있는 서로 다른 전자책 포맷이 적용되는 경우 DRM과 무관하게 호환성을 확보하기가 어렵다. 아마존은 자체의 전자책 포맷으로 AZW를 사용하는데 이 기술을 적용하는 킨들 뷰어와 애플의 iBooks처럼 IDPF ePub 표준을 준수하는 뷰어들간에는 호환성을 갖기 어렵다.

또한, 이들이 사용하고 있는 전자책 포맷이 ePub표준을 준수한다고 해도 암호화 방법이나 전자서명 같은 기술적 보호 방식이 ePub에서 권장하고 있는 W3C 기반 보호 기술이 아니고 자체적인 기술을 적용하고 있는 경우에도 호환성을 갖기 어렵다. 각각 독자적인 보호방식의 DRM기술이 적용된 ePub 콘텐츠는 암호화 키를 전달하는 방법이 표준화 되어 있더라도 암호화된 영역의 정보가 비공개이기 때문에 콘텐츠에 대한 복호화가 불가능해 진다.

2.2 상이한 권리정보의 표현방법 사용

사용자에게서 전자책의 이용허락을 위해 발급되는 라이선스에 상이한 권리정보가 사용될 경우 서로 다른 DRM기술간 상호운용성을 제공하기가 어렵다. 현재 ePub표준에서는 권리정보 표현을 위한 REL(Rights Expression Language) 기술규격이 명확하게 정의되지 않고 있다. REL의 표준화는 기술적인 문제보다는 IDPF 참여사들의 이해 관계상, 특히 단일 표준 정의에 따른 각사의 특허문제로 분쟁화의 원인이 된다. IDPF에서는 권리 정보를 저장하기 위한 파일이름인 right.xml만을 정의하고 있다. 따라서 전자책 서비스업체들이 사용하는 권리정보 표현 및 형식에 통일성을 규정화하고 있지않아서 ePub이라는 표준이 존재함에도 전자책에 대한 저작권 보호기술이 각각 사용될 경우 전자책 열람 장치들인 뷰어에 대한 호환성을 기대하기가 어렵다.

2.3 상이한 ePub 프로파일 사용

전자책 서비스 업체들이 사용하는 전자책 포맷이 ePub표준을 준수하고 기술적 보호 방식도 IDPF에서 권장하고 있는 W3C에 기반한 보호기술을 사용해도 표준에서 권고한 암호화 알고리즘의 프로파일이 보안적인 이유와 자사의 정책적인 이유로 각기 다르게 사용될 경우 상호 호환성에서 문제가 될 수 있다. 가령, NIST의 권고안에 따라 전자서명에 사용되는 암호화 수준을 RSAWIthSha256이상으로 유지하고자 하는 업체와 일반적인 RSAWithSha1을 사용하고자 하는 업체가 있는 경우, 두 업체에서 사용되는 해당 알고리즘들을 모두 지원하지 않게 되면 전자책의 호환은 불가능하게 된다. 국내에서는 암호화 알고리즘으로 SEED알고리즘을 사용할 수 있는데, 이 경우 AES 방식을 사용하는 DRM업체의 뷰어에서 열람이 불가능할 수도 있다. 마찬가지로, 전자서명이나 키 암호화에 사용되는 인증서의 경우에도 인증서의 용도 등에 대한 프로파일을 공유하지 않으면 상호호환이 근본적으로 어렵게 된다[1,10,11].

2.4 상이한 라이선스 발급 프로토콜 사용

상기에서와 같이 DRM관련 전자책 서비스 업체에서 사용하고 있는 전자책 포맷이 ePub표준을 준수하고 기술적 보호방식도 IDPF에서 권장하고 있는 W3C기반의 보호 기술을 사용하며, 표준에 대한 동일한 프로파일을 사용한다고 해도 두 서비스 사업자간에 라이선스를 발급하는 프로토콜이 호환되지 않으면 호환성을 확보하기가 어렵게 된다.

3. Solutions for Non-interoperability of eBook DRM

3.1 비표준 전자책 포맷 및 보호기술 사용

전세계의 표준으로 사용되는 전자책 포맷을 ePub표준에 따르도록 하며, 전자책의 기술적 보호조치로 사용되고 있는 보호기술은 ePub표준에서 규정하는 W3C방식의 암호화 및 전자서명방식을 준수한다.

3.2 상이한 권리정보표현 방법 사용

IDPF의 ePub표준에서는 REL에 대한 표준을 규정하지 않고 있는데 REL에 대한 표준제시가 없이는 전자책 DRM의 궁극적인 호환성을 확보하기가 어렵다. 따라서 단일 표준의 REL기술 규격을 정의해서 통일적으로 사용하는 것이 필요하다.

3.3 상이한 ePub 프로파일 사용

IDPF 표준에서 정의하고 있는 암호화 표준인 encryption.xml과 전자서명 표준인 signatures.xml 표준에서는 각기 W3C XML Encryption과 W3C XML Signature표준을 준수하도록 권고하고 있다. 그러나 이들 W3C 표준에 대한 해석과 적용 알고리즘의 다양성으로 인해 ePub보호기술 표준에 따라 개발된 현재 다수의 상용 전자책 DRM 솔루션들간에 상이한 형태를 보이고 있다. 이를해결하기 위해서는 W3C XML Encryption과 W3C XML Signature표준에서 권고하고 있는 선택항목 등을 축소하여 프로파일을 정의할 필요가 있다. W3C XML Signature표준에서는 비대칭방식의 암호화 및 전자서명을 위해 인증서의 사용이 권장되는 바, 이를 위해 인증서 표준으로 국제적으로 제정된 X.509표준에서 구현 기술의 다양성을 축소하고 안전한 프로파일로 정의할 필요가 있다.

3.4 상이한 라이선스 발급 프로토콜 사용

IDPF표준에서는 전자책 보호를 위해 사용되는 라이선스로 암호화 정보, 전자서명 정보, 권리정보등의 전달방식을 전자책을 생성할 때 전자책에 attached license인 라인선스 삽입방식을 권장하는데 복수의 DRM 클라이언트에서 보호된 전자책이 사용되기 위해서는 라이선스가 전자책과 분리되어 전달되는 방식인 separated delivery license가 요구된다. 이를 위해 DRM 서버와 DRM클라이언트 간에 라이선스를 요청하고 수락할 수 있는 프로토콜에 대한 표준 제정이 필요하다.

4. Derived Standard Elements of ePub for Interoperability

다음 Table 4.1에서는 전자책 DRM 호환을 위해 고려되는 표준항목과 IDPF ePub에서 정의하고 있는 표준, 그리고 현재 시장현황과 비호환성의 원인을 제거하기 위한 표준 대상항목을 보여주고 있다[5].

Table 4.ePub DRM Interoperability Technology Specification suggested by KATS[5]

Standard Item for Interoperability			IDPF ePub Standard	Market Situation	Standard Orienttion of ePub DRM
Secure Technology	Contents Encryption	Algorithm	W3C Encode Method	W3C Encode Method/ Independent Method	W3C Encryption Profile Standard Enactment
		Data Encode Method			
		Meta Data			
	Key trans-mission	Key Encryption Algorithm			
		Transfer Format			
		Meta Data			
	Signature	Algorithm/ Key	W3C Signature Method Recomendation	W3C Signature Method	W3C Signature Profile Standard Enactment
		Authenticat ion	Non Definition	X.509	X.509 Profile Standard Enactment
Rights Information		Transfer Format	Designation of Information File Name (rights.xml)	DRM Independent Method in rights.xml File	Standard Enactment of rights.xml Structure including Multi-rights Information
		Expression Method	Non Definition	DRM Independent Method	Standard REL Enactment or Rights Terms Standard Enactment
License Acquisition Protocol			Non Definition	DRM Independent Method	Standard Protocol Enactment
Standard Compatibility Verification			Non Definition	Independent Standard Use by DRM Technic	Enactment of Standard Compatibility Verification

상기에서 살펴본 바와 같이, 비호환 원인별 해결방안에 따라 W3C 암호화 및 전자서명 표준에서 알고리즘과 메타데이터에 대한 사용범위를 제한하는 프로파일 표준을 정의하고 인증서 사용을 위해 X.509 인증서의 프로파일 표준을 정의할 필요가 있다. 권리정보에 대해서는 권리용어에 대한 표준과 right.xml에 복수개의 권리정보를 포함할 수 있는 구조에 관련된 표준제정이 필요하며 DRM 클라이언트와 라이선스 서버간 라이선스 획득 프로토콜에 대한 표준을 제정할 필요가 있다. 또한 ePub DRM 표준을 준수하여 개발된 전자책 제작도구 및 전자책 서재

그리고 뷰어 등의 호환성을 보장하기 위해서 이들 솔루션의 표준 정합성을 검증할 수 있는 방법 및 절차에 대해서도 표준제정이 필요하다.

5. Technology Standard of ePub DRM Interoperability

ePub DRM 상호운용을 위한 기술명세로는, 암호화, 전자서명, 인증서, 권리용어 등의 관점에서 다음과 같은 표준화를 고려해야한다.[5]

5.1 암호화

ePub DRM에서 상호운용을 위한 표준화로는 ePub 표준에서 암호화 방식으로 권고하고 있는 W3C XML Encryption의 프로파일로 규정된다. 프로파일의 규정에서는 구현의 범위에 대한 축소와 보안성을 강화하는데 있다. W3C 표준에서 사용되는 암호화 알고리즘과 키 길이, 키 저장방식이 다양한 방식으로 사용되므로 W3C Encryption표준을 그대로 사용하면 보안 취약성이 있는 알고리즘과 키 길이가 사용될 수 있어서 보안의 허점이 존재할 가능성이 있다[10]. 따라서 서비스 제공업체 마다 각기 다른 명세서를 기반으로 DRM솔루션을 개발하므로 W3C표준이 포괄적으로 적용할 수 있는 다양한 구현기술명세 기반의 제품을 개발하기가 어렵다. 이러한 문제를 해결하기 위해서 데이터 암호화와 키 암호화 부분에서 다음 Table 5.에서와 같이 프로파일을 정의한다.

Table 5. Encryption Specification Profile

Item	Major Regulation Content		Type
Data Encryption	Symmetric Key	Algorithm AES-128 or more	Necessitation
		Algorithm AES-128-CBC	Recommendation
	Reference through Retrieval Method		Necessitation
Key Encryption	Non-Symmetric Key	Algorithm RSA-2048 or more	Necessitation
		Algorithm OAEP Method	Recommendation
	Symmetric Key	Algorithm AES-128 or more	Necessitation

5.2 전자서명

전자서명은 ePub 표준에서 전자서명 방식으로 권고하고 있는 W3C XML Signature의 프로파일로 규정된다. 이 프로파일에서의 규정근거는 구현범위에 대한 축소와 보안성 강화에 있는데, 이를 위해서는 다음 Table 6.에서와 같이 전자서명의 표준으로 서명정보, 키 정보, 서명대상정보 부문에서 프로파일로 정의하고 있다.

Table 6. Signature Specification

Item	Major Regulation Content		Type
Signature Information	Algorithm	RSA-SHA256	Necessitation
	Transform	Algorithm C14NWithoutComment	
	Hash	Algorithm SHA256	
Key Information	X.509 Certificate Use		Necessitation
Signature Reference Information	Transform	Algorithm C14NWithoutComment	Necessitation
	Hash	Algorithm SHA256	

5.3 인증서

인증서는 ePub 표준을 기반으로 하는 전자책 DRM 기술을 구현함에 있어 키 전달과 전자서명을 위해 사용되는 인증서에 대한 규정을 하고 있다. ePub DRM 인증서 명세서는 ITU-T의 X.509 프로파일로 구성되어 있고, 다른 표준과 동일하게 구현범위에 대한 축소와 보안성 강화에 있다. X.509포맷은 사용할 수 있는 알고리즘 및 형식이 다양하므로 범용 표준으로 적용하는데 구현 및 검증에서 매우 복잡하다. 또한 알고리즘 종류 및 비도 등에서 구체적이지 않아 보안에 취약한 알고리즘과 비도가 사용될 가능성이 있으므로 다음 Table 7.에서 인증서 저장방식, 기본 필드, 확장필드 등에 대한 프로파일을 정의한다.

Table 7. Authentication Profile

Item	Major Regulation Content		Type
Storage Method	Encoding	ASN.1 DER	Necessitation
	File Format	ASCII File : PEM	
		Binary : DER	
Basic Field	Version	V3	Necessitation
	Signature Algorithm	SHA256withSHAEncrytion	
	Serial No.	64bit Size Positive Integer	
	Issuer	DnQualifier Use	
	Subject	DnQualifier Use	
	Public Key Info.	Key Size : 2048bit	
		Exponent : 65537	
	Validity	Same as the Current Standard	
Extension Field	Key Usage	Certificate Issue, Certificat Sign, for Key Encryption	Necessitation
	Basic Constraints	CA Classification	
	Certificate Authority KeyID	CA Key ID for Certificate Issue	
	Other Extension	Prohibition on use of Critical mark	

IV. The Proposed eBSS Architecture

1. eBook Service System Architecture

1.1 eBSS의 주요기능과 DRM 적용

본 연구에서 제안하는 시스템은 Fig. 1.에서 보는 바와 같이 출판사의 책에 대한 VOD 영상과 전자책의 관리와 사용자의 전자책 구매를 효과적으로 지원하기 위한 ePub시스템을 기반으로한 eBSS시스템으로 구성되어 있다[2,3].

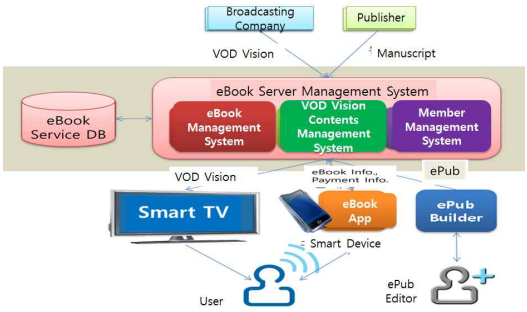

Fig. 1. System Architecture of eBSS

제안된 eBSS시스템의 주요기능은 전자책 서버관리 시스템으로 전자책관리 시스템, VOD영상 콘텐츠 관리 시스템 그리고 회원관리 시스템으로 구성된다. 또한 서버에서 제공하는 전자책을 제작하기 위한 ePub Builder가 스탠드 얼론으로 지원되며, 최종 사용자 단말기인 스마트폰에서 앱으로 지원된 전자책 앱을 통해 구매된 전자책을 리더기로 볼 수가 있게 된다. 서브시스템별 주요 기능은 다음 Table 8.과 같다[2,3].

Table 8. Major Function of eBSS

Sub-System		Major Function
eBook Server Manage-ment System	eBook Management System	-Author Management -Publisher Management -Book Management -Encrypted ePub& Encryption Key Management -Smart TV & Communication Socket Module for App. Interface -eBook Push Information
	VOD Vision Contents Management System	-VOD Vision Contents Management for Book Introduction of Terrestial Broadcasting & Cable Broadcasting -VOD Vision Watching Management
	Member Management System	-Member Information Management -eBook Purchase History
ePup Builder		-ePub pre-format Generation -ePub Generation -ePub Editing -Encryption Key Generation & ePub Encryption -ePub Viewing
eBook App.		-VOD List Viewing -TV Broadcast Content & VOD Vision Viewing -Preview & Outline of eBook (eBook Reader) -Page Preview of eBook -Purchase Process of eBook -eBook Whole Page Viewing (eBook Reader)

시스템은 크게 세 가지로 서브시스템인 전자책 서버관리 시스템, ePup Builder, 전자책 앱으로 구성된다. 전자책 서버관리 시스템은 전자책 서비스를 위한 기본적인 콘텐츠와 정보를 관리하기 위한 것으로, 저자, 출판사, 책의 원고, 암호화된 ePub과 암호화 키를 관리하는 전자책관리 시스템, 정규 방송사, 케이블 방송사, 종편 방송사의 책 소개용 VOD 영상을 관리하는 VOD 콘텐츠관리 시스템, 회원의 기본 정보와 VOD 시청 및 전자책 구매 이력 등의 정보를 관리하는 회원관리 시스템으로 구성된다. ePub Builder는 책의 원고들에 대해 ePub 생성을 위한 pre-format 생성, ePub 3.0을 준수한 ePub 파일 생성, ePub의 수정과 저장을 위한 ePub 편집, 암호화 키 생성 및 DRM을 적용하여 암호화된 ePub 제작, 그리고 ePub 파일을 읽는데 사용된다. 전자책 앱은 사용자가 관심 있는 전자책에 대한 개요 및 암호화가 되지 않은 ePub 파일의 미리 보기를 거쳐 구매하고, 암호화된 ePub 파일의 다운로드와 암호 해제 후에 전문을 보게 한다[2,3].

1.2 eBSS의 ePub Builder를 통한 DRM 적용

eBSS 시스템에서는 기본적으로 전자책의 콘텐츠를 구매하여 사용자가 서버에서 제공된 콘텐츠를 스마트폰의 전자책 뷰어기를 통해 구독할 수 있는 환경을 기반으로 한다. 여기서 ePub 빌더는 도서의 원고를 바탕으로 ePub 3.0표준을 기반으로 제작한다. Fig 2.에서와 같이, ePub을 생성하기 위한 HTML형태의 pre-format파일을 생성하고, ePub 파일을 생성하는 빌더에서 그 파일을 불러 ePub 파일을 생성시키고 저장한다. 이들 파일들은 ePub파일 편집기능을 이용하여 수정 및 편집을 수행할 수 있고, 최종 완성파일에 대해 암화화 키를 생성하여 ePub파일을 암호화하며 이 파일을 읽어 들이는 뷰어 즉 리더기를 이용하여 복호화된 파일을 읽을 수 있게 한다.

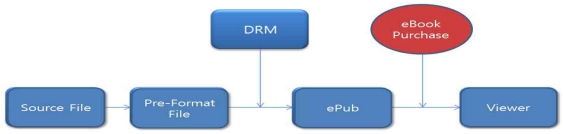

Fig. 2. Procedures of ePub Contents and the Viewer

1) ePub Builder

eBSS의 ePub Builder는 전자책 콘텐츠제작을 위한 ePub용 pre-format 생성모듈을 통해 MS Word 등의 문서 파일을 ePub 생성을 위한 파일형식으로 변환시킨다. 변환된 파일은 ePub 생성기를 통해 OCF (Open container Format) 3.0을 준수한 ePub용 파일을 최종 생성한다[2,3].

2) eBSS DRM 모듈

Pre-format용 파일을 편집하고 적용할 DRM은 ePub 파일 전체를 암호화하고, 구독자가 미리 읽어 볼 수 있는 책에 관한 정보인 '일부 보기' 기능 등과 같은 기능은 DRM 없이 제공할 수 있게 한다[2,3].

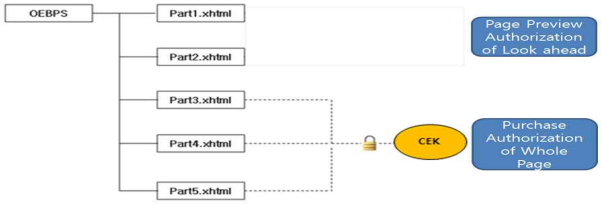

Fig. 3. Producing and Matching CEK of ePub Contents

Fig 3.에서처럼, ePub 구성 요소들의 CEK (암호화 키) 생성과 매칭을 위해서, ePub의 OCF(OEBPS Container format) 표

준 규격에 부합되는 전자책 DRM에 있어서 콘텐츠 패키징과 디패키징의 CEK(암호화 Key) 방식 암·복호화 기술을 적용한다.

여기에는

① ePub 포맷 기반 DRM 패키징에서 CEK 암호화 적용 기술 적용

② 콘텐츠, Key 암·복호화의 대칭키 알고리즘 적용 및 무결성 검증

③ CEK와 암호화된 ePub의 구성요소(XHTML, JPG, CSS 등)의 맵핑을 통한 추출과 분석 및 복호화 기술 적용

④ 복호화된 Stream의 Renderer 처리와 전자책 Viewer 모듈에서의 사용 권한 획득 및 맵핑 기술을 적용한다.

3) eBook 구매처리 DRM 연계 모듈

eBook구매처리를 위해서는 eBook 구매자에 한해 CEK 생성과 관리 및 License 발급을 위한 서버 시스템으로 사용자 인증 모듈과 전자책 콘텐츠 관리 모듈 시스템을 연계한다[13].

4) eBook ePub 리더기

스마트폰을 이용하여 구매된 콘텐츠를 볼수 있는 리더기로써 ePub 뷰어를 사용하는데 여기에는 My서재, 검색, 책갈피, 책장 넘기기, 페이지 수 resizing 등의 기능을 JAVA로 구현했다. 따라서 본 eBSS에서는 스마트기기용 eBook 책 보기와 DRM없는 eBook 책 내용 미리 보기를 구분하여 사용 권한에 따라 미리 보기는 '일부 보기'로 DRM이 없는 전자책으로 제공할 수 있게 하였다. eBook 주문처리와 관련된 전자결제는 제3자 전자결제서비스 업체와 연계 처리하도록 되어 있다.

eBook 보기는 사용 권한에 따라 구매 절차에 의하여 '전체보기'는 DRM을 해제할 수도 있도록 융통성 있는 기능을 구현하도록 스마트폰 Android환경하에서 개발하였다.

2. USE CASE and Class Diagram of eBSS

2.1 ePub Builder USE CASE와 eBook 보기 USE CASE

운영자는 ePub Preformat 형식으로 원본 문서를 저장하고 ePub 파일을 생성한다. 생성된 ePub 파일을 ePubBuilder를 통해 읽고 편집한 후 암호화를 적용한다. 적용된 암호화에 대한 키와 암호화된 ePub 파일을 서버에 저장한다.

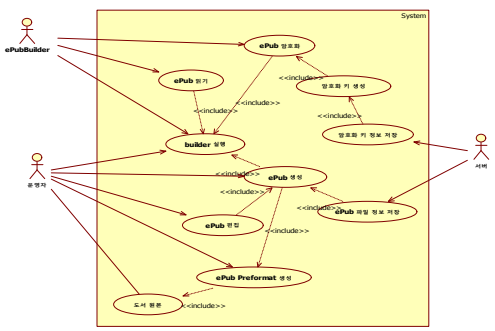

Fig. 4. USE CASE of ePub Builder

사용자가 앱을 실행하여 전자책 개요를 보고 전자책에 대한 전문을 본다. 전자책 개요를 보기 위해서는 서버와 통신을 하며, 서버에서 갖고 있는 전자책 개요 정보를 사용자에게 보여준다. 앱은 전자책 복호화를 담당하고 사용자는 전자책 전문을 볼 수 있다.

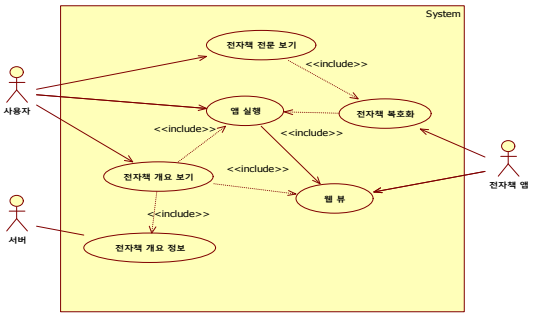

Fig. 5. USE CASE of eBook Viewer

2.2 ePub Builder와 전자책 앱의 클래스 다이어그램

전자책 제작과 ePub용 DRM적용을 위한 클래스 다이어그램은 다음 Fig 6.과 같고, 전자책 앱용 클래스 다이어그램은 Fig 7.에서 보는 바와 같다.

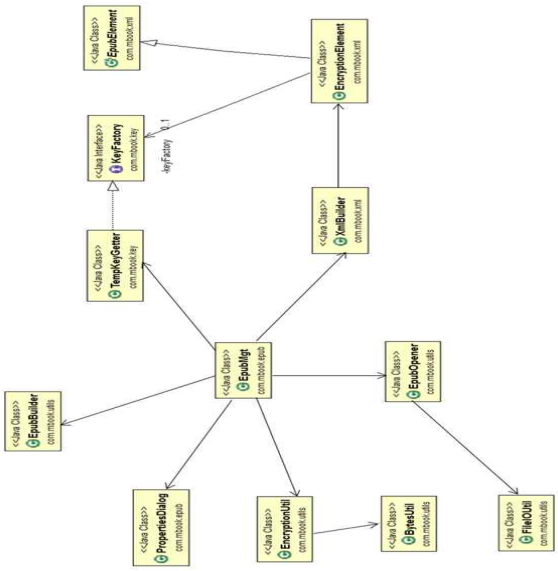

Fig. 6. Class Diagram of ePub Builder

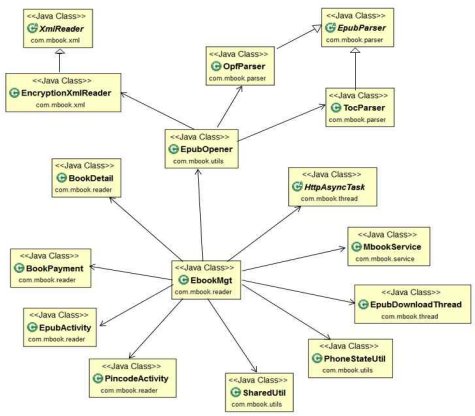

Fig. 7. Class Diagram of eBook App. for Smart Phone

3. Sequence Diagrams of ePub Builder

3.1 ePub 파일 TreeView 생성

운용자는 ePub 파일의 편집을 위해 Fig 8.과 같은 TreeView 생성 과정을 통해, ePub 파일의 구조를 보고 편집을 할 수 있도록 ePub 확장자 내부의 목록을 메모리에 할당한다. TreeView 생성 과정은 ePubBuilder의 기초 과정으로 ePubBuilder의 모든 과정은 TreeView 생성 과정이 선행되어 있음을 전제로 한다. TreeView 생성 과정의 흐름은 다음과 같다.

①ePubBuilder 관련 프로그램 실행
②출력된 화면을 보고 편집할 ePub관련 파일 선택
③선택된 ePub 파일의 내용을 내부로직을 통해 메모리에 할당
④사용자에게 보일 TreeView를 생성 후 화면에 표출

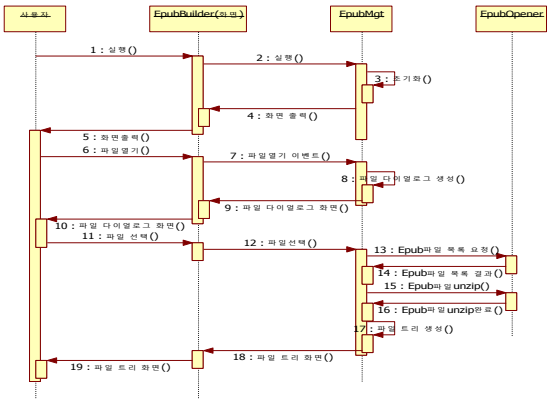

Fig. 8. TreeView Generation of ePub File

3.2 ePub 원본 파일 보기

운용자는 ePub 파일이 포함하고 있는 각각의 파일에 대한 원본 소스의 내용을 있는 그대로 화면에서 볼 수 있다.

파일 소스 화면 출력 과정은 다음과 같으며 Fig. 8.의 TreeView 생성 과정이 선행되어 있음을 전제 조건으로 한다.

①MBookMgt 클래스에서 TreeView에 SelectionListener를 등록
②SelectionListener에서 운용자가 TreeView를 선택할 경우 선택된 파일에 대한 정보를 요청
③FileIOUtil을 통해 파일의 내용을 읽어 MBookMgt에 전달
④운용자 화면에 파일 내용을 할당

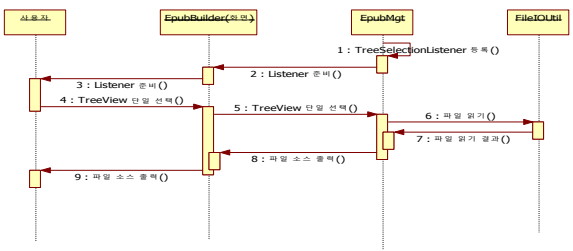

Fig. 9. Reading an ePub Source File

3.3 전자책 보기

운용자는 ePub 파일이 포함하고 있는 각각의 파일이 전자책 화면에서 어떻게 표현되는지 알려면 전자책 기능을 통해 확인할 수 있다. 전자책 화면 출력 과정은 다음과 같으며 TreeView 생성 과정이 선행되어 있음을 전제 조건으로 한다.

①MBookMgt 클래스에서 TreeView에 SelectionListener를 등록
②SelectionListener에서 운용자가 TreeView를 선택할 경우 선택된 파일에 대한 정보를 요청
③전자책 뷰어의 초기화 후 해당 내용을 전자책 화면에 출력

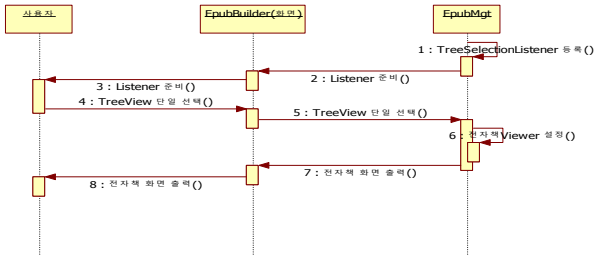

Fig. 10. Reading an eBook

3.4 암호화 Tree 생성

운용자는 ePub파일을 배포할 경우, 무단(불법)복제를 방지하기 위하여 암호화 기능을 통해 파일 내용을 암호화할 수 있다. 암호화 트리 생성 과정은 다음과 같으며 Fig. 10.의 TreeView 생성 과정이 선행되어 있음을 전제로 한다.

①운용자가 암호화 메뉴를 선택
②현재 열려있는 ePub 파일에서 암호화할 목록을 읽어온다.
③암호화 모듈 초기화를 진행하고 암호화할 데이터의 암호화를 진행
④암호화가 완료되면 암호화된 데이터(Byte Array 형태)를 Base64기반 인코딩을 진행한다.
⑤XmlBuilder 객체를 생성하여 encryption.xml(데이터를 암호화할 경우, ePub 국제 규격을 따르기 위해 반드시 존재해야하는 파일) 파일을 생성한다.
⑥암호화된 데이터 목록을 참고하여 TreeView에 목록을 생성한다.

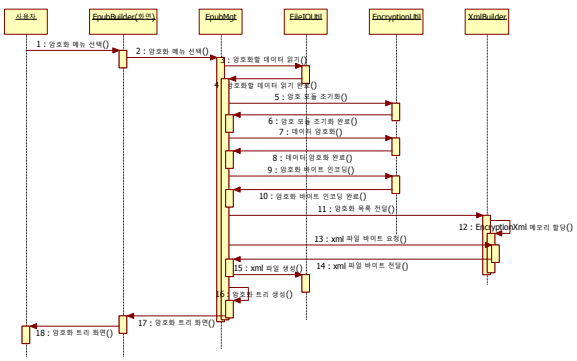

Fig. 11. Generation of Encryption Tree

3.5 복호화 Tree 생성

운용자는 암호화된 ePub 파일의 내용이 이전과 다른지 확인

하기 위해 복호화 기능을 통해 파일 내용을 확인할 수 있다.

복호화 트리 생성 과정은 다음과 같으며 Fig. 11.의 암호화 트리 생성 과정이 선행되어 있음을 전제로 한다.

①운용자가 복호화 메뉴를 선택한다.
②메모리에 할당되어 있는 암호화 데이터 목록을 읽어온다.
③암호화 모듈 초기화를 진행한다.
④암호화된 데이터를 원본 데이터 형식(Byte Array 형태)으로 가져오기 위해 Base64기반 디코딩을 진행한다.
⑤암호화 원본 데이터를 복호화 한다.
⑥복호화된 데이터 목록을 참고하여 TreeView에 목록을 생성한다.

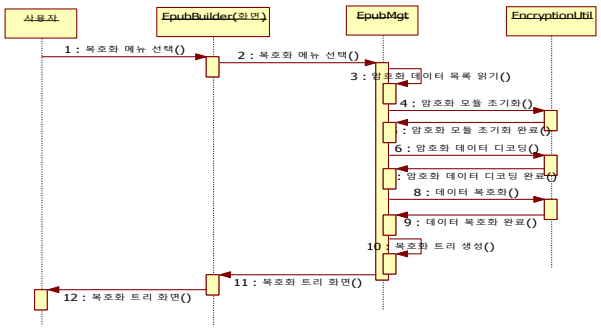

Fig. 12. Generation of Decryption Tree

3.6 전자책 개요 및 미리보기

사용자는 전자책을 구매하기 앞서 전자책에 대한 개요(미리보기)를 볼 수 있다. 전자책 개요의 시나리오는 책 목록 보기의 과정이 정상적으로 처리되고 책에 대한 시퀀스 값이 항상 존재한다는 것을 전제로 한다.

①사용자가 전자책을 선택한다.
②선택된 전자책에 대한 시퀀스 값을 객체에 저장한다.
③사용자에 대한 정보를 조회하여 객체에 저장한다.
④HttpAsyncTask 클래스의 객체를 생성하고 인자로 전자책 개요 요청에 대한 데이터를 넘긴다.
⑤전자책 개요를 서버에 요청한다.
⑥서버는 사용자 인증 후 전자책 개요 정보를 앱에 전송한다.
⑦앱은 전달받은 데이터를 확인하여 오류가 발생했는지 확인한 후, 정상적인 정보일 경우 전자책 개요 화면을 사용자에게 보여준다.

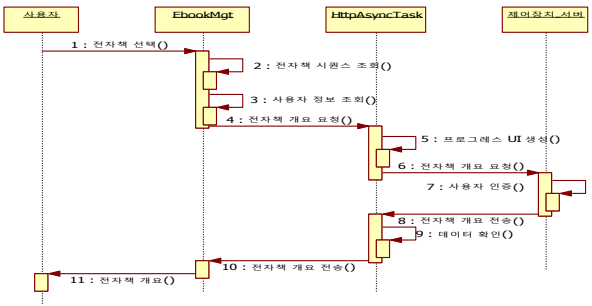

Fig. 13. Preview Pages of eBook

3.7 전자책 내려받기

사용자는 전자책 전문을 보기 위해 최초 한 번 이상의 내려받기 기능을 수행하여야한다. 전자책 내려받기 시나리오는 사용자가 최소 1권 이상의 책을 구매하고 My 서재의 시나리오를 거쳤다고 가정한다. 또한 구매한 책은 내려받기가 되어있지 않은 상태인 것을 전제로 한다.

①사용자가 보고 싶은 전자책을 선택한다.
②앱이 사용자에 대한 정보를 조회한다.
③ HttpAsyncTask를 통해 전자책에 대한 정보를 서버에 요청한다.
④서버는 사용자 인증 후 전자책에 대한 정보를 앱에 전송한다.
⑤앱은 전자책에 대한 정보를 받아온 후, 사용자에게 데이터 이용 요금에 관한 정보를 화면에 표시한다.
⑥사용자가 승인을 할 경우, EpubDownloadThread 객체를 생성하여 전자책 내려받기를 요청한다.
⑦EpubDownloadThread는 전자책에 대한 정보에 들어온 URL을 통해 Stream을 생성하고 전자책 내려받기를 수행한다.
⑧내려받기가 진행되는 동안 프로그레스 UI를 화면에 표시하여 사용자가 내려받기 상황을 알 수 있도록한다.
⑨전자책 정보를 통해 전자책과 전자책 복호화에 대한 key를 내려받고 파일을 내부 저장소에 저장한다.

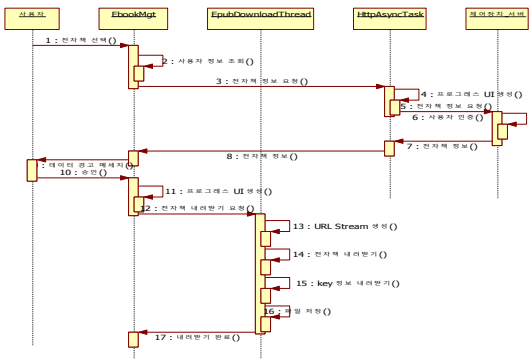

Fig. 14. Downloading of eBook Contents

3.8 전자책 전문 보기

사용자는 구매한 전자책의 전문을 Reader를 통해 볼 수 있다. 전자책 전문 보기 시나리오는 사용자가 최소 1권의 책을 구매하고 구매한 책의 내려받기를 완료한 상태라고 가정한다.

①사용자가 보고 싶은 전자책을 선택한다.
②선택된 전자책에 대한 시퀀스를 조회한다.
③EpubLayout 객체를 생성하고 화면 생성을 요청한다.
④EpubLayout은 보여줄 화면에 대한 초기화를 수행하고 EpubOpener 클래스에 전자책 파일을 요청한다.
⑤EpubOpener에서 전자책 파일을 읽어 데이터 파싱을 수행하고 정상적으로 파싱이 완료되면 데이터를 EpubLayout으로 전달한다.
⑥EpubLayout은 전자책의 복호화를 EpubOpener에 요청한다.

⑦EpubOpener는 전자책이 암호화된 전자책인지 확인하고 암호화가 되어있다면 복호화하여 복호화된 전자책 데이터를 EpubLayout에 전달한다.
⑧EpubLayout은 화면을 구성하기 위해 InitPageThread에 페이지 생성을 요청한다.
⑨InitPageThread는 전달받은 정보를 토대로 페이지를 생성하며 최대 페이지 등의 정보를 확인하고 EpubLayout에 전달한다.
⑩EpubLayout은 페이지에 대한 정보를 통해 사용자가 보고 있는 페이지 화면을 불러와 보여준다.

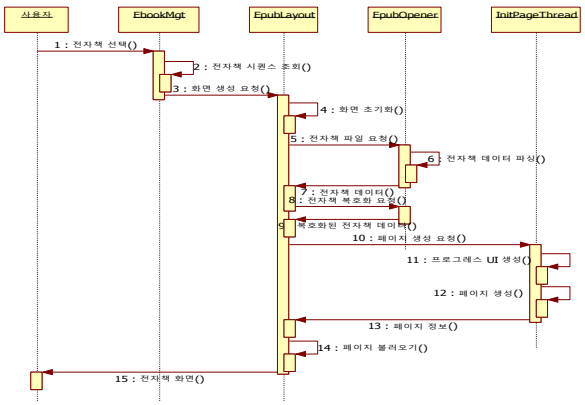

Fig. 15. Reading of the Full eBook Contents

V. The Prototype System of eBSS

다음은 메타생각이란 전자책을 통해 DRM 생성과정을 적용해 본다. 실제로 5권의 DRM생성과 복호화 과정을 통해 ePub 제작과 생성 및 복호화를 통해 뷰어기에서 100% 완성률을 보였다.

1. Pre-Format File Generation

1.1 ePub-preformat

먼저 사용자는 preformat 형식으로 바꿀 원본 파일을 다음과 같이 텍스트 파일로 준비한다.

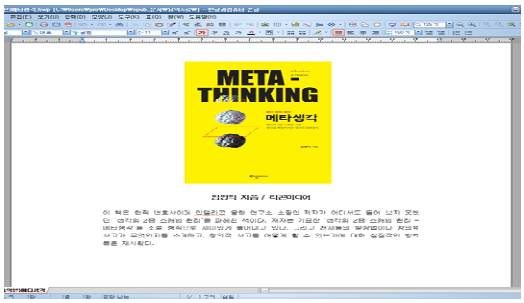

Fig. 16. Screen of ePub Pre-format

1.2 html 파일 생성

ePub preformat으로 생성된 파일을 불러서 html형식의 파일로 변환한다.

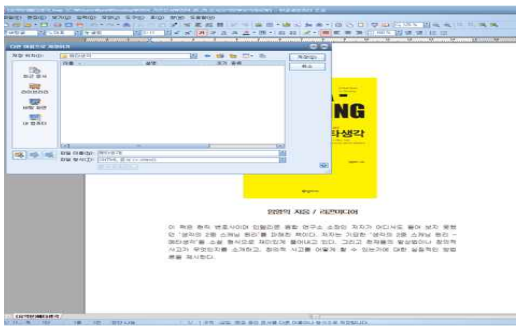

Fig. 17. Screen of HTML Generation for ePub Pre-format

2. ePub Editor

2.1 ePub 편집기에서 html 파일 로드하는 화면

ePub편집기에서는 ePub preformat으로 생성된 html파일을 불러서 다음과 같이 ePub파일로 생성한다.
다음은 ePub편집기에서 ePub파일을 생성하는 화면이다.

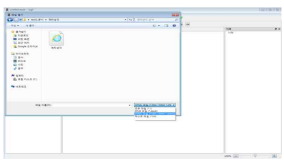

Fig. 18. Screen of Opening HTML File

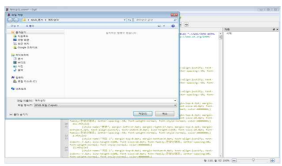

Fig. 19. ePub File Generation

2.2 ePub 파일의 구조를 보기 위한 TreeView 생성 화면

ePub파일의 구조를 TreeView로 보여주고 이를 통해 해당 파일의 구조를 볼 수 있다.

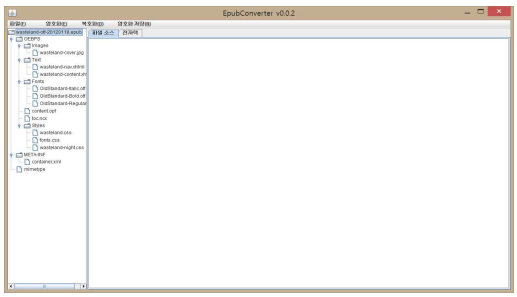

Fig. 20. TreeView of ePub File Structures

2.3 ePub파일의 실제내용(원본 소스)을 보는 화면

생성된 ePub파일의 실제 소스파일을 화면에서 볼 수 있다.

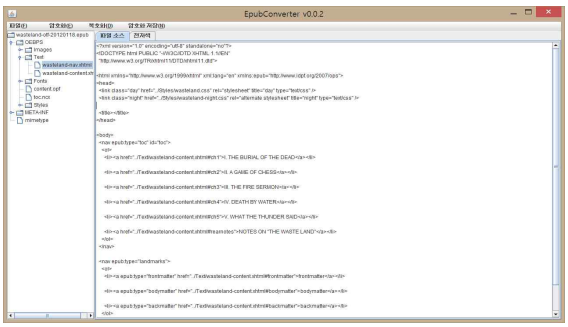

Fig. 21.ePub Source File

2.4 ePub 파일이 사용자에게 보이는 모양을 미리 보는 화면

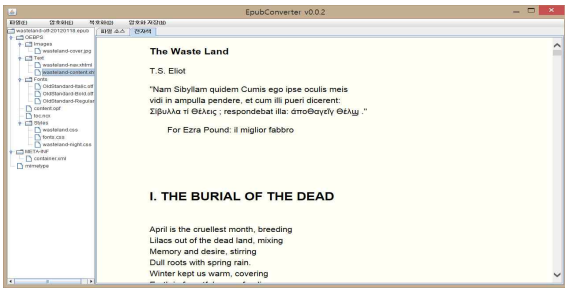

Fig. 22. eBook Contents

최종 생성된 ePub파일을 뷰어기의 형식을 빌려 실제 내용을 보는 화면이다.

3. DRM 생성

3.1 암호화 Tree

ePub 파일을 암호화하여 암호화된 파일에 대한 구조를 보기 위한 TreeView 생성 화면이다.

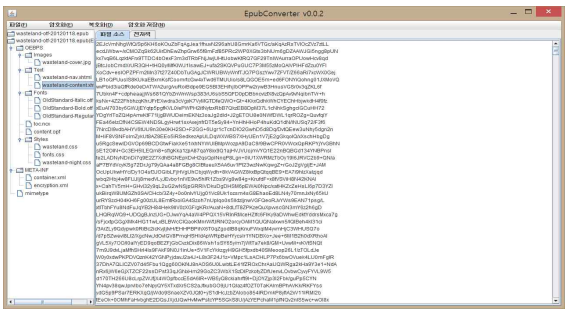

Fig. 23. Encryption Tree

3.2 복호화 Tree

암호화된 ePub 파일을 복호화하여 생성된 파일에 대한 구조를 보기 위한 TreeView 생성 화면이다.

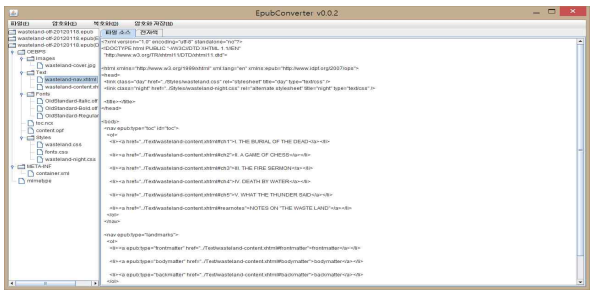

Fig. 24.Decryption Tree

4. 전자책 보기 뷰어

4.1 최종 DRM해제된 전자책 보기 (전자책 복호화)

복호화된 ePub이 사용자에게 보이는 내용을 미리 보는 화면이다.

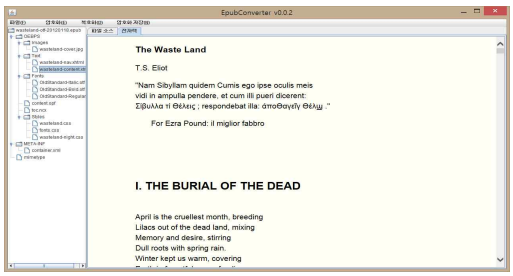

Fig. 25. Viewer Screen of the Decripted eBook Content

4.2 eBook 다운로드 진행과정

ePub 파일 다운로드 시 진행 상태를 보여주는 화면이다.

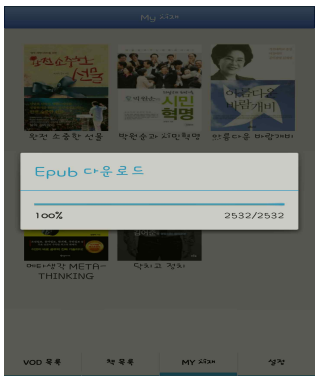

Fig. 26. Screen of Downloading eBook

4.3 eBook보기(책장 넘기기와 페이지 수 resizing)

다운로드된 ePub을 복호화 하여 전문을 보여주는 화면으로 새로운 페이지에 맞게 리싸이징을 하는 기능을 넣어서 책장을 넘기는데 필요한 페이지의 재설정이 가능하다. 따라서 eBook 보기에서 글자 크기를 변경하면 자동으로 페이지가 재설정된 화면이 나타난다.

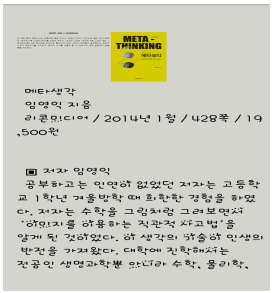

Fig. 27. Screen of the Full eBook Contents Viewer and Page Eject

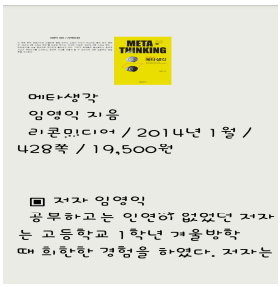

Fig. 28. Page Resizing of eBook Viewer

4.4 eBook보기(키워드 검색기능 과 책갈피기능)

다음은 eBook보기를 통해 다양한 단어를 검색할 수 있는 화면으로 eBook 보기에서 '수학'이라는 키워드를 검색하여 나온 화면이면 Fig. 에서는 책갈피 기능을 이용하여, eBook 보기에서 책갈피를 한 후 보여지는 내용을 화면에 표시한 것이다.

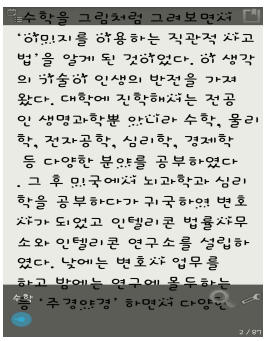

Fig. 29. Keyword Search of eBook Contents

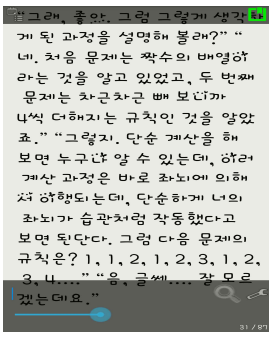

Fig. 30. Book Mark Screen of eBook

VI. Evaluations and Conclusions

본 연구에서는 범용적인 전자책을 제작하기 위한 ePub빌더를 개발하였고, 여기에 산업체에서 공통으로 적용할 수 있는 ePub 3.0기반의 최적 표준 DRM을 적용할 수 있는 기능과 이를 복호화 해서 전자책 뷰어기로 구독할 수 있는 eBSS 시스템을 개발하였다.

eBSS 서비스 시스템은 서버측 관리를 위한 TV 방송콘텐츠 관리시스템, eBook관리시스템, 회원관리시스템으로 구성되는 eBook 서비스 서버가 있고, eBook 편집자를 위한 ePub Builder, 사용자를 위한 eBook App으로 구성되어 있으며, 또한, ePub 콘텐츠의 저작권보호를 위한 암호화 알고리즘의 적용과 암호화된 콘텐츠의 복호화를 위한 DRM 적용 기법을 실증적으로 제시하였다.

본 eBSS에서 생산된 콘텐츠를 다양한 리더기상에서 관련 eBook의 내용을 뷰어로 손쉽게 볼 수 있는 ePub 빌더시스템의 리더기에 적용될 효율적인 DRM을 적용했다. 또한, 향후 적용될 기준을 국내 공통 표준으로 적용하기 위해서, 국가 기술표준원의 표준안을 채택하여 IDPF의 ePUB 3.0에서도 무리없이 적용할 수 있는 최적의 전자책 DRM을 실제 전자책의 제작과정에 적용하였다.

최적의 전자책DRM 적용을 위한 eBSS의 프로토타입 시스템을 이용하여 사용자에게 시스템 퍼포먼스에 대한 테스트를 실시하였다. 참여자인 20명의 사용자에게 직접 전자책 제작과 DRM을 적용한 후 복호화 하여 ePub뷰어를 통해 실제 내용을 읽게 하였다. 참여자들은 eBSS시스템의 사용자 만족도를 설문을 통해 측정하게 하였다. 여기서 주요기능 요소들로는 사용의 편의성, DRM적용성, 전자책리더기인 뷰어기의 기능성으로 하였고, 다음과 같이 각 요인별로 리커트의 5점척도(①매우 만족, ②만족, ③보통, ④불만족, ⑤매우 불만족)로 체크하게 하고 이를 다음 Table 9.에서와 같이 실증분석을 하였다. 각 문항당 최고 5점 최저 1점의 리커트 스케일로 하였다. eBSS시스템의 전자책 서비스 제공자와 전자책 사용자 관점에서 실시한 결과 다음과 같다.

Table 9. Performance of Major Function of eBSS

	eBSS ePub Builder and Factors of Major Function			Measure-ment Scale
	Usability	DRM Applica bility	Viewer Functionality	Lickert 5 Scale n=20
Average	4.21	4.70	4.87	

Table 9.에서 보면 뷰어기의 기능성이 page resizing과 북마크, 검색기능 등으로 가장 만족도 평균이 높았고, DRM의 적용이 비교적 용이하며 융통성있게 적용이 가능해 두 번째로 높았다. 반면 사용 편의성은 4.21로 만족스럽긴 하지만 전자책 제작과 사용에 대한 전반적 이해의 부족에 기인하는 것으로 사료된다.

본 연구는 스마트 시대에 부합하는 ePub 콘텐츠의 생산과 분배 및 복제에 있어서 최적화된 기술로 디지털 콘테츠의 저작권 보호를 위한 암호화 및 복호화 처리 절차를 위한 방법과 시스템을 제시하였다. 그러므로 기존의 다양한 서책을 ePub화 하고, 사용자의 요구에 맞는 전자책 콘텐츠를 서비스 하는데 적용할 수 있는 효과적인 DRM기법으로 산업적 파생 효과가 기대된다. 향후 연구에서는 범용적인 전자책 제작과 DRM적용의 최적화된 전자책 저작도구로써 범용적인 활용도를 높이고, ePub빌더의 유용한 도구가 될수 있도록 시장에서의 요구기능을 확대 적용한 보편화된 ePub 제작도구로써의 기능연구를 수행할 예정이다.

REFERENCES

[1] Kyoung-Ok Cho, "Design and implementation of packaging mechanism for protection of DRM

contents in Mobile environment," Journal of Korean Institute of Information Technology, Vol.8, No. 9, pp. 77 - 86, 2010.

[2] Eung Sup Jun, and Yong Sik Chang, "An eBook Service System based on VOD Broadcasting Contents of Smart TV," Journal of The Korea Society of Computer and Information, Vol. 19, No. 12, pp. 257-266, December 2014.

[3] Eung Sup Jun, Yong Sik Chang, Sang Soo Oh, Yun Eui Choi, "A Framework for Hybrid eBook Service System based on Mobile Smart Device and Smart TV Broadcasting Contents," The KSCI Summer Conference 2014 pp. 45-48, July 2014.

[4] Yeongh Hun Yi, Chang Ha Choi, Kyo Young Chin, and Sung Wook Joe, "DRM applying method for ebook service based on EPUB standard," Computer Aided Publishing Society, Jounal of digital Publish, Vol.1, No. 1, pp. 79 - 84, 2012.

[5] The Korean Agency for Technology and Standards, “Specification for Interoperable KS ePub DRM,“ 2014.

[6] Dong Eun Kim, Nah-yeon Ahn, and Kyoung-Ryul Lee, "Consideration of necessity to standardize the e-book DRM," The Korea Entertainment Industry Association Spring Conference 2014 pp. 194-202, May 2014.

[7] Ho-Gap Kang, Tae-Hyun Kim, Hee-Don Yoon, and Seong-Hwan Cho, "A Study of ePub-based Standard Framework Supporting Mutual Comparability of eBook DRM," Journal of The Institute of Internet, Broadcasting and Communication Vol.11, No. 6, December 2011.

[8] W3C, “XML Encryption Syntax and Processing Version 1.1,” 11 Apr. 2013, Last accessed 15. Oct. 2014.

[9] International Digital Publishing Forum, http://idpf.org/epub/3.0, Last accessed 15. Oct. 2014.

[10] Sang Chul Kim, Hyung Ku Kang and Hee Yong Youn, "A Proposal on Secure Partial Encryption for Mobile Digital Rights Management," The Korean Institute of Communications and Information Sciences, Autumn Conference 2012, pp. 414 - 415, 2012.

[11] Jong-Won Yang, Mi-Young Kim, Chang-Ho Seo and Heang-Suk Oh, "Analysis and Design system of contents partial encryption for Mobile DRM environment," Journal of The Korea Entertainment Industry Association Vol. 3, No.2, pp. 22-28, 2009.

[12] Yeon-Soo Choo, Young-Ku Lee and Moon-Seog Jun, "Design Secure Key of Decryption Distribution System for DRM System," The Korean Institute of Information Scientists and Engineers, KCC 2005 Tutorial Vol. 32, No.1(A), pp. 157-159, July 2005.

[13] Eun-Bum Kim, Kyung-Il Kim, Tae-Hyeun Kim, and Seong-Hwan Cho, "A Study of Partial Preview Control Method of ePub-based eBook DRM," Journal of The Institute of Internet, Broadcasting and Communication Vol.12, No. 1, December 2012.

Authors

Eung Sup Jun received the M.S. degree in Computer Science and Engineering from Yonsei University, and received Ph. D. degree in Intelligence Information System from KAIST. He received a certificate of Software Engineering Evangelist program from the School of Computer Science, Carnegie Mellon University in USA. Dr. Jun worked for KAIST System Engineering Research Institute as a researcher from 1985 to 1989, and worked for HP korea as a system consultant from 1989 to 1991. He joined the faculty of the Department of Computer Software at Induk University, Seoul, Korea, in 1991. He is currently a Professor in the Department of Computer Software, Induk University. He is interested in mobile web and app. system development and IoT application based on Intelligent Information System.