Journal of Korea Multimedia Society Vol. 14, No. 12, December 2011(pp. 1601-1612)

Process Analysis of Digital Right Management for Web-Based Multicast Contents

Wildan Toyib[†], Man-Gon Park[††]

ABSTRACT

In recent years, advanced in digital technologies have created significant changes in the way we reproduce, distribute and market Intellectual Property (IP). DRM for multicast contents is complicated risk, the further technology development and human demand, this approaching is still being researched by the scientist and all by the company which is conducting in piracy management reduced, and every country has national policy to make this consortium to limit piracy properties, based on this paper research development, just only two approaching to reduce piracy in DRM they are Industrial Property (IP) and Copyright. In this paper, we are not only figuring and analyzing about the processes to reduce and limit the piracy and unprotected copy law but also describing about the encryption process, watermarking and digital signature process algorithms. The basic concepts of this encryption process for web-based multicast content in DRM are implemented in Java. We conduct this method is a computerized through web based application system approaching to reduce unprotected copy and piracy. Which is used in DRM for multicast content in every section, by providing a fundamental in information technology development, we believe this research is reliable to prove that is unprotected copy, and piracy can be reduced by protecting with this paradigm.

Key words: Digital Right Management (DRM), Web-Based Multicast Contents, Encryption Process, Intellectual Property (IP)

1. INTRODUCTION

Digital Rights Management (DRM) technology is the core system that allows the owners to distribute their films in a controlled way. The owner specifies, in which ways and under which conditions each cinematic asset may be accessed (digital rights, licensing), and the DRM system will try to ensure that each asset can only be accessed as specified by the owner (enforcement). The same DRM system can also be used to distribute films over the Internet. For example, a film studio may specify that each film may be showed in a licensed cinema for a given period starting at a given time by codec system software application [1-3].

The content or asset we consider in this paper is newly released very high value entertainment content of a cinematic title, including video, audio but also text and metadata[4,5]. From the data management perspective, a typical two hour 35 mm feature film scanned at a standard high-quality resolution of 1920 by 1080 pixels and 24 frames per second (used for high-end HDTV as well) would, in its uncompressed form, require more than one terabyte of disk space[6]. The goal of a pirate is to obtain an unprotected copy of a given film, movies and music, which can be distributed without restriction. In the past, pirates have used a variety of distribution channels for stolen video content,

※ Corresponding Author : Man-Gon Park, Address: (608-737) 599-1 Daeyeon-Dong, Nam-Gu, Busan, Rep. of Korea, TEL : +82-51-629-6240, FAX : +82-51-628-6155, E-mail: mpark@pknu.ac.kr
Receipt date : Nov. 16, 2011, Revision date : Dec. 26, 2011
Approval date : Dec. 31, 2011
[†] Dept. of Advanced Information Science and Technology, Graduate School, Pukyong National University (E-mail: wildantoyib@pknu.ac.kr)
[††] Dept. of IT Convergence and Application Engineering, Pukyong National University, Rep. of Korea

including physical distribution (e.g., production and distribution of video CD/DVD, sometimes based on copies made with camcorders in cinemas) and electronic distribution over the internet networking[7]. Multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source creating copies automatically in other network elements, such as routers, only when the topology of the network requires it. The Encryption based technologies transform content into unintelligible forms[8,9]. This transformation is being reversible naturally, allows perfect recovery of content before consumption. Technologies based on watermarking embed data directly into the content, resulting in imperceptible degradation in visual quality. End to end security is the most critical requirement to create of new digital markets where copyrighted content is the key product of DRM [10-12].

In this paper we propose the business process models and encryption process data models for DRM system implemented in a frame work of web-based multicast contents. These models represent some fundamental concepts of protecting the resources and keys of DRM system applied in portal of web-based multicast contents.

2. RELATED WORK

2.1 Multicast Contents

Multicast enables efficient large-scale content distribution by providing an efficient transport mechanism for one-to-many and many-to-many communication. Over the years, multicast has been the topic of many research, engineering, and deployment efforts. These efforts have continued to transform multicast into a technology that can be relied on by many applications. Work has been done in reliability, manageability, scalability, quality of service (QoS), and ease of deployment. As these areas become more mature, there is increased potential for multicast to be used as the underlying distribution mechanism for content distribution applications[13]. Therefore, security in multicast content distribution is a concern. The maturity of multicast security solutions have the potential to enable the use of multicast for confidential and high value content, and help spark the use of multicast by new applications. There are a number of security issues in multicast content distribution directly related to the properties of multicast that make it efficient and attractive[14].

There has been research that provides solutions to many of these security issues. Some of these solutions are ready for deployment, some are nearing maturity, and others are only in the early phases of research. The maturity and deployment of these solutions will help increase the ability of multicast technology to deliver new applications and more content. In this article we examine these various issues and solutions for providing secure multicast content distribution, and outline several future research directions.

Multicast is a receiver based concept, receivers join a particular multicast session group and traffic is delivered to all members of that group by the network infrastructure. In a traditional system, the sender does not maintain a list of receivers. Only one copy of a multicast message passes over any link in the network, and copies of the message are made only where paths diverge at a router. Multicast packets from remote sources are relayed by routers, which forwards them on to the local network if there is a recipient for the multicast group on the LAN. The Internet Group Management Protocol (IGMP) is used by multicast routers to identify the existence of group members sending IGMP queries and having receives report their group membership. Multicast services accommodate capabilities such as mobility, bandwidth, flexibility, and security[13-15].

2.2 IP Television Multicast Distribution

An Internet Protocol (IP) television system can

distribute information through a switched telephone network. These functions show that end users are watching a movie that is initially supplied by media centre (media server) that is located some distance and several switches away from end users (movie watchers). When the first movie watcher requests the movie content, it is requested from the telephone end office through Digital Subscriber Line (DSL)[15].

The telephone end office determines that the movie is not available in its video storage system and the end office switch requests the movie from the interconnection switch. The interconnection switch also determines the movie is not available in its video storage system (main server) and the movie is requested from the distant media source. When the movie is transferred from the media centre to the end customer, the interconnecting switches may make a copy for future distribution to other users. This program distribution process reduces the interconnection requirements between the switching distribution systems, to illustrate the concept of IP television multicast distribution as depicted in Fig. 1.

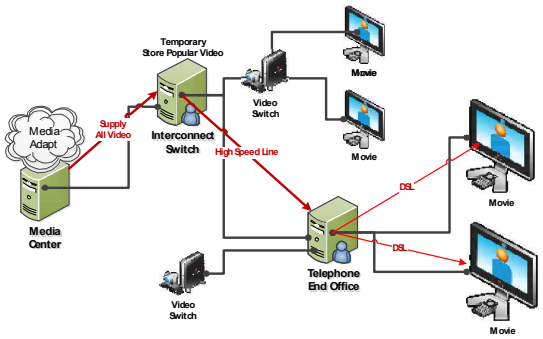

Fig. 1. IP Television Multicast Distribution.

2.3 Multicast Single Source

A single source multicast data session is to allow a single source to send the same information to multiple receivers without the need to repeat the transmission, back through multiple switches and routers in the network[16,17]. Fig. 2 shows that an IP address source is combined with a single multicast address that allows each router in the multicast tree to forward the packets only to members of the group (single source), the more detailed illustration of this figure will be shown in below.

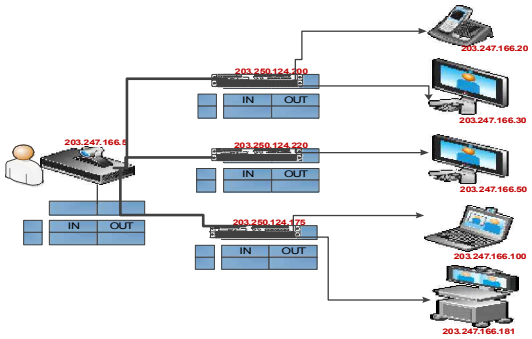

Fig. 2. Multicast Single Source.

2.4 Multicast Share Source

Multicast share source shows how a shared source multicast data session to allow multiple sources to send the information to multiple receivers through the user of a reference address (rendezvous point/RFC 2362). In this illustration, the data from each source is sent to the Rendezvous Point (RP) which then distributes the information through a tree structure to the multicast group recipients[18]. This diagram shows that there is the potential for some duplicate transmission in the shared source multicast session as the source and destination may be sent in different directions through the same routers, the Fig. 3 illustrates the process of multicast share source implementation.

3. DRM SYSTEM FOR MULTICAST CONTENTS

DRM for multicast content is a research which is never ending a couple of year. Based on the cases according to intellectual property, the international consortium applied two categories right of rules to handle covered about digital right in multicast contents. It is divided into two categories: The first (1) is industrial property which includes in-

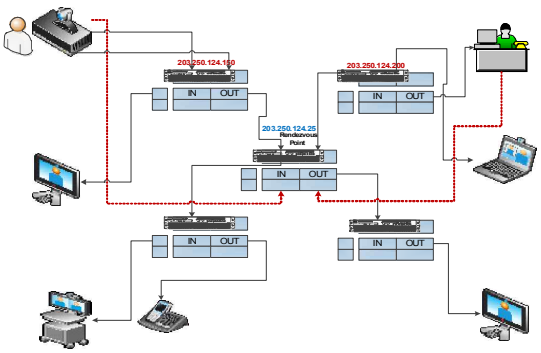

Fig. 3. Multicast Share Source.

ventions (patents), trademarks, industrial designs, brand image, scientific source, publication, prototyping, geographic indications of source, founding of great idea in social network as is Facebook, twitter etc. The Second (2) is copyright which includes literary and artistic works as are novels, both of poems and plays, films, journal, musical creation, artistic creation as is to be drawings, paintings, photographs, sculptures, and architectural designs. A multicast content is a cluster of digital audio/visual (A/V) devices including set top boxes, TVs, Internet TV, VCRs, DVD players, and general purpose computing devices such as PC, notebook, smart phone devices, and radio telecommunication infrastructure. Copyrighted digital multimedia content may be delivered to the consumers from a number of sources including the Internet, satellite, terrestrial or cable television systems. It may also be made available as prepackaged media (e.g., a digital tape or a digital video/audio disc) at retail stores. Before releasing their content for distribution, the content owners may require protection by specifying certain access conditions and Digital Rights Management (DRM) [16,17]. According to complicated matters in developing country which is for buying high quality or branded of a trade mark property license, it is limited by patents and copyright, hence the price of properties is too expensive for weak economic realm. Therefore piracy is the economic way to capture all the properties in multicast content neither in many cast demand within couple a year[18].

To limited all the piracy environment by reducing production the properties unprotecting, such as trademarks, industrial designs, geographic indications of source, novels, both of poems and plays, films, musical creation, artistic works as are drawings, paintings, photographs, sculptures and architectural designs, so DRM is a basic scientific to cover all these cases. We conduct to create an engineering approaching way, by collaborating science and technology to prove all the methods in information technology field[19].

The Fig. 4 is a diagrammatic representation of a number of real-time processes, databases and user interfaces that together provide the functionality of a conditional access server according to an exemplary embodiment of the present invention.

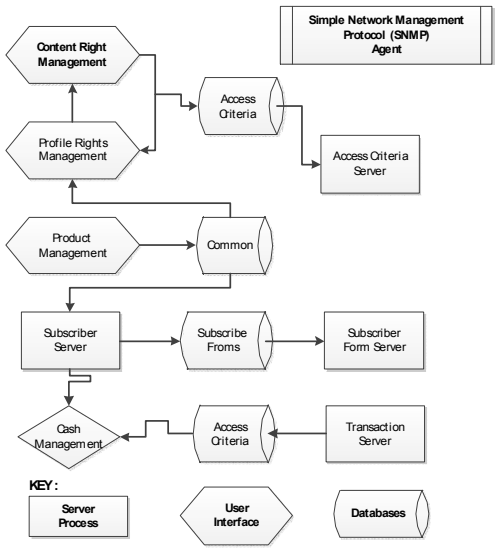

Fig. 4. Function Chart of DRM System.

4. ENCRYPTION PROCESS AND DIGITAL SIGNATURE OF DRM SYSTEM FOR WEB-BASED MULTICAST CONTENTS

4.1 Architecture of Web-Based Multicast Contents

The development process of DRM can be applied in internet application as a web based system. Fig.

5 is a block diagram illustrating further details regarding software components that may reside at various location of the content distribution system to facilitate distribution and delivery processes, according to an exemplary embodiment of the present invention, encryption is the process of transforming information (referred to as plaintext) using an algorithm (cipher) to make it unreadable to anyone except those possessing special knowledge [20], usually referred to as a key.

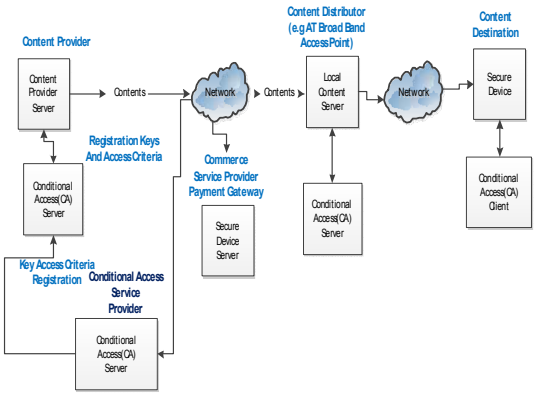

Fig. 5. Web Based Application Systems of DRM System.

In this method, we are applying simple hash function algorithm as shown in Fig. 6. It is an encryption flowchart providing further details regarding a method, according to an exemplary embodiment of the present invention of generating the digital signature for a license utilizing a symmetric key (e.g. product keys). The license is subject to a hash function generating a hash result.

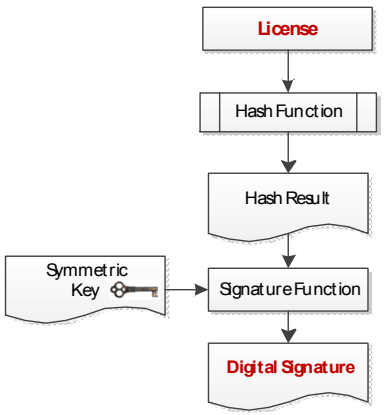

Fig. 6. Encryption Process for Generating Digital Signature.

The hash result and a symmetric key in the exemplary form of a product key provide input to a signature function that generates a digital signature for the license from these two inputs[21]. To get the product key, hash function will be verified by the symmetric key and digital signature as shown in Fig. 7.

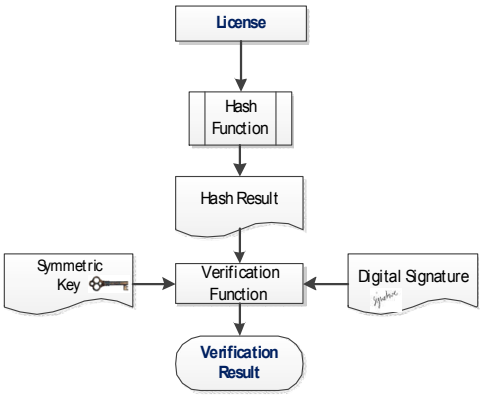

Fig. 7. Combining Process between Encryption and Digital Signature Methods.

According to an exemplary embodiment of the present invention of verifying a content license, it can be utilized by a digital signature generated utilizing a symmetric key (e.g., a product key). The license is again subject to the hash function to generate the hash result. A verification function receives the three inputs, namely the hash result, the symmetric key and the digital signature[22]. As the digital signature was generated utilizing the symmetric key. The verification function is able to verify the content license utilizing these three inputs.

The function of the Business Process Modelling (BPM) in Fig. 8 for web-based multicast content is to accumulate the effective approaching to classify the requirement of system application. The key-concept of this figure is to get direction as is methodology to be a frame work of an encryption

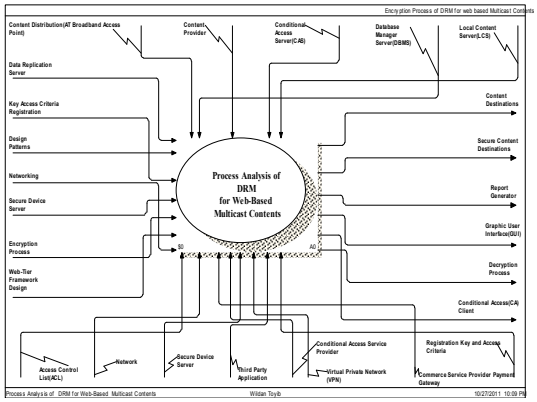

Fig. 8. Context Diagram for Business Process Modelling (IDEF0) of DRM System with Web-Based Multicast Contents.

process of DRM for web-based multicast contents. In order easy to classify the system requirement the BPM of the system above is extracted to become work flow data modelling and diagraming which is illustrated by following frame work Fig 9.

In designing content provider business process as a part of web-based multicast content, the detail extraction method is the effective way, in order to understand the algorithm of system running in deployment and code development. The Fig. 10 is an extraction process of work flow diagram is to be focusing in communication session which is configured in communication layer application.

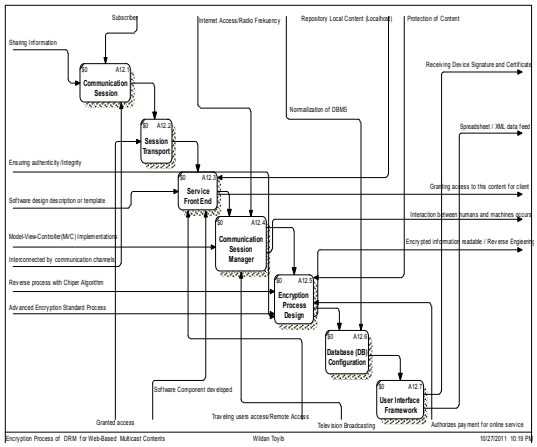

Fig. 9. Work Flow Model (IDEF3) of Encryption Process for DRM System with Web-Based Multicast Contents.

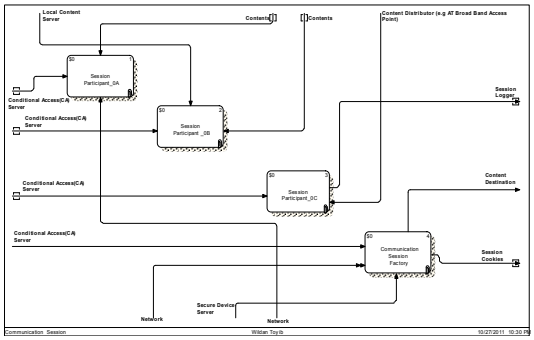

Fig. 10. Work Flow Diagram for Communication Session Part of Content Provider Business Process.

The modelling method and diagramming in session participant part of content provider business process is an extraction process from Data Flow Diagram (DFD) system from Fig. 8 in communication session layer, therefore on the Fig. 11 the modelling method and diagramming is created to extract running well in service layer details.

The decision support system to configure an encryption process of DRM system for web-based multicast content is figured on the Fig. 12, this illustration is a logical method of Data Flow Diagram (DFD), and this algorithm is using the key combination AND/OR Gate to generate verification result, finally on the output process within this layer delivery digital signature and report[23].

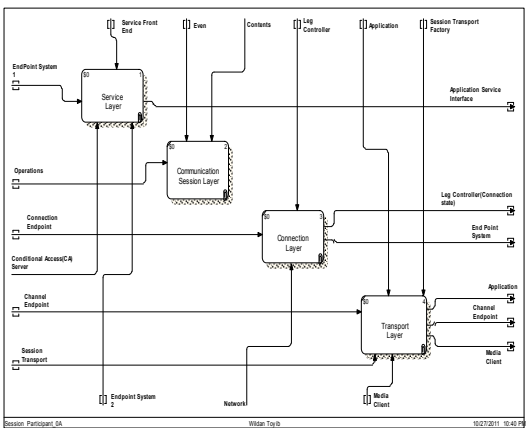

Fig. 11. Work Flow Diagram at 2nd Level for Session Participant Part of Content Provider Business Process.

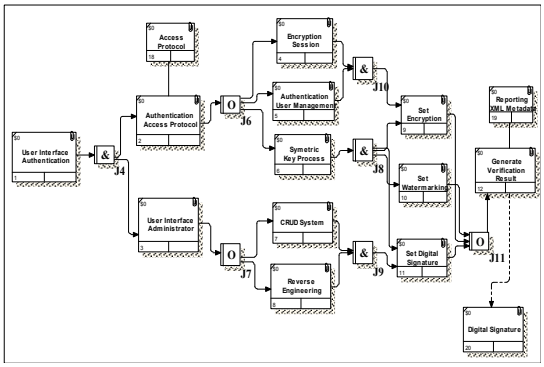

Fig. 12. Function Process Model of Service Layer in Content Provider for DRM with Web-Based Multicast Contents.

Both of this output is produced from setting of encryption, watermarking and digital signature. These processes are running in service layer application to authenticate user interface to get report of verification result on encryption process of DRM system for web-based multicast contents. Further information about this figure sees the illustrations below.

Finally, Database schema for web-based multicast content in DRM system is produced in Fig. 13. These processes are reverse engineering from business process management of this research.

The structure data for this system is according to the business process for the DRM likewise in the primary key for industrial property and copyright. We create four big tables to manage da

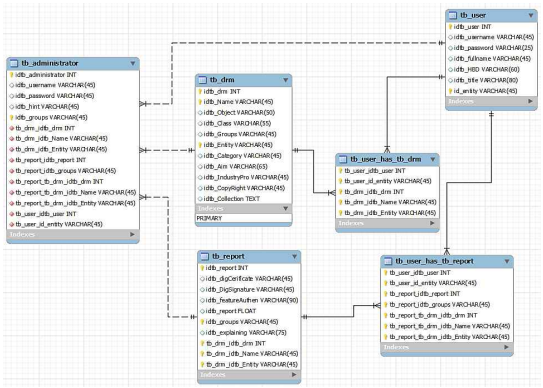

Fig. 13. Database Schema for Web-Based Multicast Contents in DRM System.

ta warehouse on this schema simplify.

We configure the simple method to build this schema, there are four table which represent, where is a web-based for DRM for multicast content can gather the input process data from the client. The CRUD (Create, Read, Update, and Delete) is responsibility of the user authority with Access Control List (ACL) privileged[24]. The main result of this function is to generate a report classification in to two categories, the first is Industrial Property (IP) and the second is copyright in web based reporting system. These database system is configure in DB designer, to produce this schema many ways to do, as to be here database configuration will be exported to XML schema. It is going to be used for SOAP entity in content provider deployment[25].

Database configuration for this system is configured as pseudo-code logic below; in this web-based system we apply to use an enterprise Oracle DB Server. So then the Structure Query Language (SQL) is the answer for this method. The following is the database connection URL syntax: jdbc:db_drm:[subsubprotocol:] [databaseName] [;attribute=value]*, subsubprotocol specifies where command should search for the database, either in a directory, in memory, in a class path, or in a JAR file[29,30]. It is typically omitted. Database name is the name of the database to connect to. Attribute equal to value represents an optional, semicolon-separated list of attributes. These attributes enable to instruct database to perform various tasks, including the following: Create the database specified in the connection Uniform Resource Locater (URL), Encrypt the database specified in the connection URL, Specify directories to store logging and trace information and Specify a user name and password to connect to the database[25,26].

On the other hand to limit increasing entry data until the space limitation is reached. We implement an algorithm to execute the views related to the query1, query2, query3, and query4. The ratio of

the query processing the two categories[29], the ratio of the query processing property in data warehouse to the database could be calculated through formula 1. In this formula the benefit of removing the pre-process to extract and transform some fields (such as industrial property and copy-right group) are relinquished.

The ratio of the query processing property can be written by

$$R_{QP} = \frac{\sum_i S_i}{\sum_i P_i}, \quad (1)$$

where P_i is the processing property of the i^{th} query (q_i) on the database and S_i is the processing property of the i^{th} query (q_i) on the data warehouse. The number of records in a table which are accessed to answer a query has direct effect on P_i and S_i. The numerator of this formula is 1.9*108, and the denominator is 6.6*108. Therefore query processing improves about 3.5 times, and the proposed roadmap was used to choose the most suitable algorithm for view selection to decrease query response time.

4.2 Web-Based Architecture

Web-based architecture describes an infra-structure that enables a web-based system or application to achieve its business objectives. In this research, in the Fig. 14, we implemented the Model-View-Controller (MVC) Architecture; this pattern is used to optimize the reliability of the system as an object oriented methodology based on the case of the DRM system for web-based multicast contents[30].

4.3 Content Provide Entities Procedure

A content provider entity represents one eXtensible Markup Language (XML) source from a specific content provider (database DRM schema). The entity provides all the information required for making a connection with the content provider and

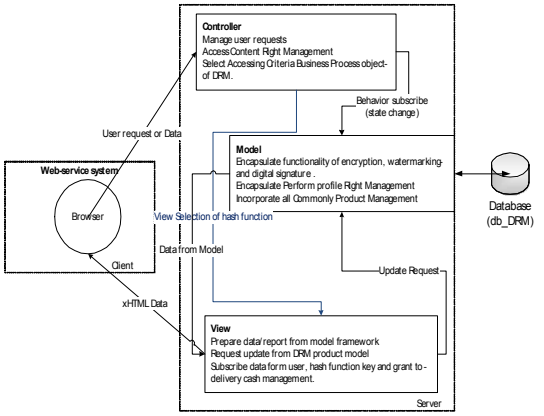

Fig. 14. The Model-View-Controller (MVC) Architecture of the DRM system for Web-Based Multicast Content.

retrieving the specific XML source. Several entities can be implemented by the same Java class. There are two types of entities, first is Hypertext Transfer Protocol (HTTP) Entity: An entity that obtains XML via an HTTP request. And the second is Simple Object Access Protocol (SOAP) Entity: An entity that obtains XML via a SOAP request[28]. On the other hand, in this method, we will perform the creating SOAP entities only; on this case the web-based for multicast content in DRM includes an *AbstractSOAPProviderEntity* class that implements all required methods of *IProviderEntity* and *ITransformationProviderEntity* interfaces in order to make SOAP requests. We need to implement the *createRequestMessage()* method, which returns the SOAP message as defined in the content provider's Web Services Description Language (WSDL) [28]. Table 1 can be shown the creating SOAP entities information as the pseudo code.

This pseudo code can be completed if necessary through override *doInit()* method, also *getGeneral-Parameters()* method. These methods define parameters that are passed to all the transformers associated with this entity.

5. CONCLUSIONS

In recent years, advanced in digital technologies

Table 1. Creating SOAP entities information as the pseudo code

```
{
    // Create SOAP Envelope
    SOAPMessage msg = createBasicEnvelope();
    SOAPEnvelope env =
   msg.getSOAPPart().getEnvelope();
    SOAPBody body = env.getBody();
    // Create GetNewsstandHeadlines Element
    SOAPElement getNewsStandHlElement =
   body.addChildElement(
   env.createName("GetNewsstandHeadlines","",
          ICPService.CP_NS_DEV2_1_PARSERS));
    // Create sectionIDs Element
    SOAPElement sectionIdsElm =
       getNewsStandHlElement.addChildElement(
       env.createName("sectionIDs","",
          ICPService.CP_NS_DEV2_1_PARSERS));
    // Create sectionID Element
    SOAPElement sectionIDElm  =
   sectionIdsElm.addChildElement(
       env.createName("sectionID","",
          ICPService.CP_NS_DEV2_1_PARSERS));
    // Create Section Code
    sectionIDElm.addTextNode(
   m_sourcePropertiesHandler.getParameterValue(
          m_request,"sectionCode"));
    return msg;
}
```

have created significant changes in the way we reproduce, distribute and market Intellectual Property (IP). Digital media can now be exploited by the IP owners to develop new and innovative business models for their products and services. In a world where piracy is a growing potential threat, the rights of the IP owners can be protected using three complementary weapons: technology, legislation, and business models. Because of the diversity of IP (eBooks, songs and movies), no single solution is applicable to the protection of multimedia products in distribution networks through internet networking. IP is created as a result of intellectual activities in the industrial, scientific, artificial, literary and artistic. It is divided into two categories: (1) Industrial property - includes inventions (patents), trademarks, industrial designs, brand image, scientific source, founding, geographic indications of source, and (2) Copyright - includes literary and artistic works such as novels, poems, films, publications, musical works, artistic creation as is drawing, painting, photograph, sculpture, and architectural design. A multicast content is a cluster of digital audio/visual (A/V) devices including set top boxes, TVs, VCRs, CD/DVD players, and general-purpose computing devices likewise PC, notebook and smart phone. Copyrighted digital multimedia content may be delivered to the consumers from a number of sources including the internet, satellite, terrestrial or cable television systems. Recently, three fundamental groups of technologies in Digital Right Management (DRM) are; encryption, watermarking, and digital signature have been identified for protecting copyrighted multimedia content in digital distribution networks. The web-based multicast contents with authentication system from three of these technologies are a key-concept for this research, the effective methodology for these cases are performed through business process, work flow, data modeling and diagramming details. End to end security is the most critical requirement to create of new digital markets where copyrighted content is the key product.

REFERENCES

[1] Darko Kirovski, Marcus Peinado, Fabien A. P. Petitcolas, "Digital Right Management for Digital Cinema," *Journal of Multimedia Systems*, Vol.9, No.3, pp. 228-238, 2003.

[2] Refik Molva, Alain Pannetrat, "Network Security in the Multicast Framework," *Lecture Notes in Computer Science*, Vol.2497, pp. 481-485, 2002.

[3] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," *Lecture Notes in Computer Science*, Vol.1109, pp. 1-15, 1996.

[4] M. V. D. Burmester and Y. Desmedt, "A Se-

cure and Efficient Conference Key Distribution System," *Lecture Notes in Computer Science*, Vol.950, pp. 275-286, 1995.

[5] Bellare, M., Desai, A., Jokipii, E., Rogaway, P, "A Concrete Security Treatment of Symmetric encryption," *Proceedings of IEEE Foundations of Computer Science*, pp.394-403, 1997.

[6] Robert W. Fransdonk, "Method and System to Secure Content for Distribution via a Network," *United States Patent No.6961858-B2*, appl. No.10/321,767, 2005.

[7] Morin, J. H., Konstantas, D., "Commercialization of Electronic Information," *Proceedings of IEEE International Conference on Multimedia Computing and Systems*, Vol.2, pp. 524-529, Jul. 1999.

[8] Schneier, Bruce, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., (1996), 2nd Edition, pp. 31-32, 2001.

[9] Schneier, Bruce, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., Chapters 2 and 3, pp. 21-74, 1996.

[10] Chae Duck Jung, Weon Shin, Young-jin Hong, and Kyung-hyune Rhee, "Interval Two-Dimensional Hash Chains and Application to a DRM System," *Journal of Korea Multimedia Society*, Vol.10, No.12, pp.1663-1670, 2007.

[11] Judge, P. Ammar, M, "Security Issues and Solutions in Multicast Content Distribution: a survey," *Proceedings of IEEE on Network Security*, pp. 30-36, 2003.

[12] Cheriton, D. Deering, S, "Host Groups: A Multicast Extension for Datagram Internetworks," *Proceedings of the ninth symposium on Data communications,* pp.172-79, 1985.

[13] Deok-Gyu Lee, Hyung-Geun Oh, and In-Young Lee, "A Study on DRM Model Using Electronic Cash System," *Journal of Korea Multimedia Society*, Vol.7, No.8, pp.1107-1119, 2004.

[14] Ballardie, T, Crowcroft, J., "Multicast-Specific Security Threats and Counter-Measures," *Proceedings of IEEE of Network and Distributed System Security*, pp. 2-16, 1995.

[15] Judge, P. Ammar, M, "Gothic: A Group Access Control Architecture for Secure Multicast and Anycast," *Proceedings of IEEE Computer and Communications Societies*, pp. 1547-1556, 2002.

[16] Chung Kei Wong. Lam, S.S, "Digital Signatures for Flows and Multicasts," *IEEE/ACM Trans. on Networking*, pp. 502-513, 1999.

[17] Rohatgi, P, "A Compact and Fast Hybrid Signature Scheme for Multicast Packet Authentication," *Proceedings of the 6th ACM conference on Computer and communications security (CCS '99)*, New York, pp.93-100, 1999.

[18] Canetti, R. Garay, J. Itkis, G. Micciancio, D. Naor, M. Pinkas, B, "Multicast Security: A Taxonomy and Some Efficient Constructions," *Proceedings of IEEE Computer and Communications Societies*, pp. 708-716, 1999.

[19] Brown, I., C. Perkins, J. Crowcroft, *Watercasting: Distributed Watermarking of Multicast Media*, NGC, 1999.

[20] L Vicisano, L Rizzo and J Crowcroft, "TCP Like Congestion Control for Layered Reliable Multicast Data Transfer," *Proceedings of IEEE Infocom Transaction*, 1997.

[21] Ballardie, T., Crowcroft, J., "Multicast-Specific Security Threats and Counter-Measures," *Proceedings of IEEE Symposium on Network and Distributed System Security*, pp. 2-16, 1995.

[22] S. Chuang, Jon Crowcroft, S. Hailes, Mark J. Handley, N. Ismail, D. Lewis, I. Wakeman, "Multimedia Application Requirements for Multicast Communications Services," *Proceedings of International Networking Conference (INET'93)*, Barry Leiner (Ed.), San

Francisco, California, pp. 1-9, 1993.

[23] Jingwen J., Nahrstedt, M, "mc-SPF: An Application-Level Multicast Service Path Finding Protocol for Multimedia Applications," *Proceedings of IEEE International Conference on Multimedia and Expo (ICME2002)*, Vol.1, pp. 765- 768, 2002.

[24] Jun Yao, Anjun Zhao, Lei Guo, "A Movel Video Multicast Instant Source Authentication Model Based on Digital Watermarking and TESLA," *Proceedings of International Conference on Communication Technology (ICCT 2003)*, Vol.2, pp. 1719- 1722, 2003.

[25] Moyer, M.J., Rao, J.R., Rohatgi, P., "A Survey of Security Issues in Multicast Communications," *IEEE Trans. on Network*, Vol.13, No.6, pp. 12-23, 1999.

[26] Calvin E. Lewis, "Multimedia Communication Management System with Subscriber Message Integration Services," *United States Patent Application Publication*, 2002.

[27] Hinard, Y., Bettahar, H., Challal, Y., Bouabdallah, A., "AAA Based Security Architecture for Multicast Content Distribution," *Proceedings of International Symposium on Computer Networks*, pp. 85-90, 2006.

[28] Ian Wakeman and Jon Crowcroft, "Multicast Congestion Control in the Distribution of Variable Bit Rate Video," *Technical Report of the Computer Science Department, University College London*, 1994.

[29] Daneshpour, N., Abdollahzadeh Barfourosh, "Data Engineering Approach to Efficient Data Warehouse: Life Cycle Development Revisited," *Proceedings of International Symposium on Computer Science and Software Engineering (CSSE2011)*, pp. 109-120, 2011.

[30] Roger S. Pressman, *Software Engineering A Practioner's Approach*, Seventh Edition, McGraw Hill, International Edition, 2010.

Wildan Toyib

He received engineering degree in computer science with Class Honors from Institut Teknologi Sepuluh Nopember in 2007. He has completed M.S degree course in Advanced Information Science and Technology, Graduate School, Pukyong National University, Republic of Korea. He has experience in the IT field such as Team Lead of Programmer for Electronic Data Processing from 2007-2008 and as Senior IT Reporting for Chevron Corp. in Energy Component for ideSIDE server report environment IndoAsia Business Unit from 2008-2009. He worked for The Ministry of National Education, Republic of Indonesia with BERMUTU (Better Education Through Reformed Management Universal Teacher Upgrading) which is supported by World Bank and Netherland Government from 2009-2010. He is member of IAENG and student member of IEEE. His research interests include safety and security of ubiquitous computing systems, ubiquitous sensor networks, software reliability engineering, data engineering, multimedia information processing technology and web and internet technology.

Man-Gon Park

He is a head professor of the Dept. of IT Convergence and Application Engineering, College of Engineering, Pukyong National University, Republic of Korea since 1981. Also he was the president and vice president of the Korea Multimedia Society (KMMS). He served as the Director General and CEO of the Colombo Plan Staff College for Technician Education (CPSC) from 2002 to 2007, which is an intergovernmental international organization of 29 member governments for Human Resources Development in Asia and the Pacific Region. He served there also as a faculty consultant seconded by the Government of the Rep. of Korea as an expert in information systems development and ICT-based TVET systems from 1997 to 2001. He has been the visiting professor at the Department of Computer Science, University of Liverpool, UK; exchange professor at the Department of Electrical and Computer Engineering, University of Kansas, USA; and visiting scholar at the School of Computers and information science, University of South Australia. He was dispatched to Mongolia and People's Rep. of China by KOICA on various projects as information systems consultant. He has also embarked on consulting works and conducted training programs in ICT on individual capacity for Korean groups of companies, governmental and non-governmental agencies and other institutions in Korea. His main areas of research are software reliability engineering, business process reengineering, Internet and web technology, multimedia information processing technology, system performance evaluation, and ICT-based human resources development