IMPLEMENTATION OF STRUCTURAL DIAGRAM FOR INTELLECTUAL PROPERTY MANAGEMENT AND PROTECTION(IPMP)

Junghee Park*, Kidong Lee**, Sang-jae Lee***

Contents

Key Words:Australia, innovation, R&D, Government policy, Tax Concession

Abstract

While Internet promises ubiquitous access, it also creates a fundamental challenge to the traditional ownership toward digital assets traded in e-commerce market. Sharing digital information freely through shared networks leads to many untapped business opportunities, but uncontrolled digital asset transaction undermines many electronic business models. Thus, in this Internet age, proper protection and safe delivery of Intellectual Property (IP) and its representation as digital assets would be a crucial ingredient of building trust in upcoming e-business environment. In this paper, we give a general structural diagram of Intellectual Property Management and Protection (IPMP) and implement an IPMP prototype based on the RSA encryption algorithm and XrML (eXtensible rights Markup Language) WORK tags to show how proper protection and safe delivery of the intellectual property is achieved. This study concludes that IPMP mechanism may contribute significantly to the volume and quality of e-commerce market.

* Department of Information Technology, Jaeneung College, Incheon, South Korea
jpark@jnc.ac.kr
** School of Business, University of Incheon, Incheon, South Korea
kdlee@incheon.ac.kr
*** School of Business, Sejong University, Seoul, South Korea

I. INTRODUCTION

While Internet promises ubiquitous access, it also creates a fundamental challenge to the traditional ownership toward digital assets traded in e-commerce market. Sharing and copying valuable information freely in the Internet and e-commerce space may not fit with the traditional concept of ownership of goods, especially when applied to digital assets. In this "information society" where power and wealth increasingly depend on information as key assets, protection and management of intellectual property (IP) would be a crucial ingredient toward new e-business model[1].

Intellectual Property (IP) encompasses all the tangible and intangible products of the human capital. Some examples of such intellectual property products include music, video, games, software, and business and proprietary corporate information[2]. Recently, a lot of products themselves or contents of goods are digitalized so that their illegal downloads (or reproduction) over a long geographical area can be done instantly. Many cases of on-line frauds, hacking, and misuse of information in the current Internet make it imperative that the IPMP structure and technologies should be set up as early as possible to protect the electronic market user and simultaneously enhance the quality of service (QoS) in the Internet commerce[3]-[5].

In this paper, we give the structural diagram for the key components of an Intellectual Property Management and Protection (IPMP) mechanism so that save protection and proper deliver mechanism should be established in the e-commerce market[6][7].

Section 2 gives the brief illustration of Intellectual Property Management and Protection in terms of definitions and benefits. Section 3 shows the structural diagram of the proposed Intellectual Property Management and Protection systems and their detailed description. Section 4 provides the detailed encryption algorithm and demonstrates work tags of intellectual property right to build safe e-commerce channel. And future research and conclusion are followed.

II. INTELLECTUAL PROPERTY MANAGEMENT AND PROTECTION

2.1 What is IPMP?

Intellectual Property (IP) includes all products, digital or non-digital, made by human work. In 21 century, intellectual creativity of human capital has recognized the most valuable resource of all. Thus, IPMP technologies are designed to protect intellectual property (IP) of the user. The user here is denoted as any e-commerce participants including customer, producer, creator, distributor, etc. IPMP tries to protect IP by building a trusted market framework, a prerequisite for the success of the digital asset commerce[8][9].

Research on Intellectual Property Management and Protection (IPMP) focuses on providing safe transaction mechanism to the transitional market of the traditional market to e-commerce based the Internet and currently available network technologies[10][11]. Various technical standard groups and technical vendors (i.e., Microsoft, InterTrust, Adobe, ContentGuard) are encouraged to cooperate to set up the working models of IPMP infrastructure.

The purpose of Intellectual Property Management and Protection is to provide the complete packages of new digital commerce services that protect, create, deliver, and enhance the intellectual property (IP) of the users in the e-commerce market[12][13].

2.2 Benefits of IPMP

Among various possible benefits that IPMP provide for the establishment of the e- commerce, three important ones are protection of digital asset, protection from content manipulation, and provision for transaction & user information[14].

Protection of digital assets:

IPMP uses encryption technologies to protect the content of digital goods. This is usually done using a special key. Once digital asset is protected via IPMP encryption, only the holder(s) of this key can later unlock the content and read the content. Thus, it is quite important to properly manage keys (key management).

Protection from content manipulation:

IPMP can guard against digital manipulation, thus protecting content originality, using a one-way hash function. For example, a one-way hash function takes a digital book content of any length as input and produces a small, fixed-length output message called a message digest, which is sent to a user. If any part of the original content is changed, the altered message text will produce completely a different message digest. Thus, the user of the IPMP system knows whether the message has been changed during the transfer period.

In electronic markets, a business contract between content sellers and buyers is sealed with digital signatures[15]. Thus, the business contract is protected from others. Another way of protecting a digital contract is to use watermarking technologies[16]. Watermarking is an encryption technique where patterns of bits are intentionally embedded into a digital document in a way that is invisible to others, but can be read by special programs. With the use of several technologies just mentioned above, the original digital asset is protected from data manipulation.

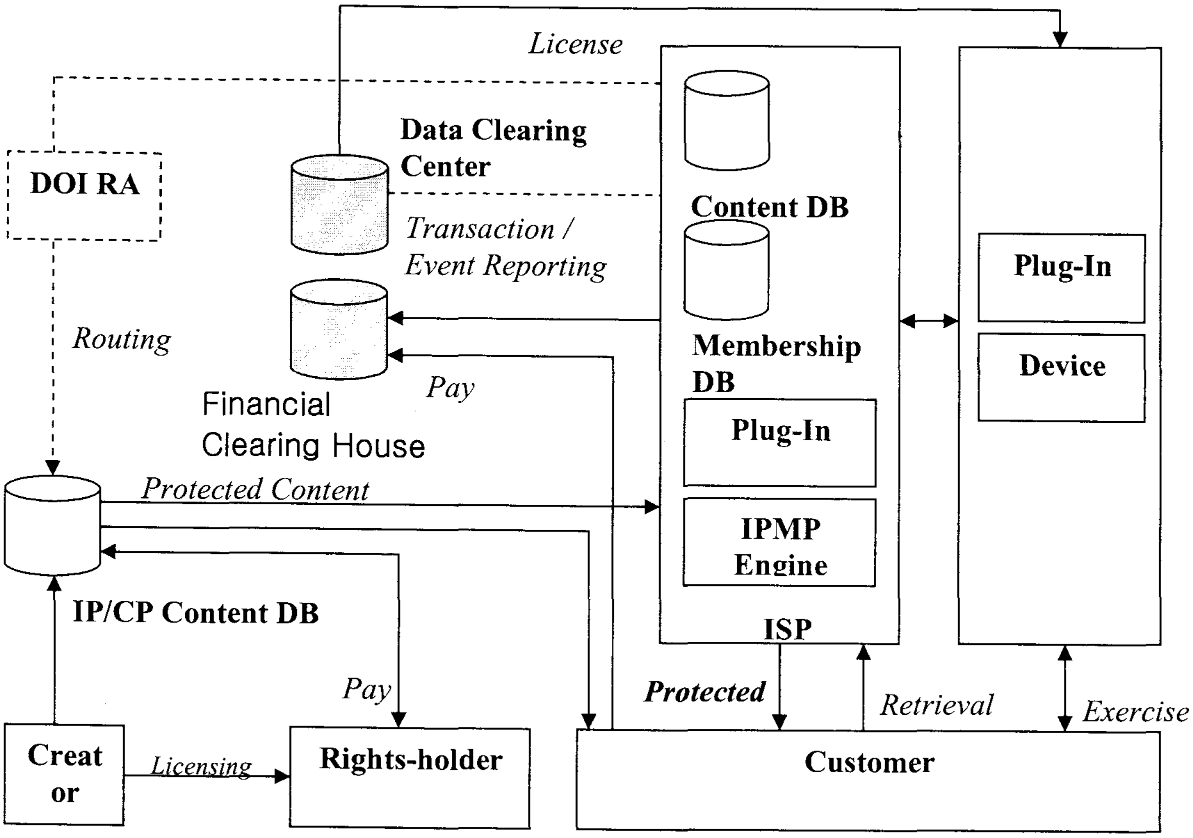
Provision for transaction & user information

Once the business contract is made and successfully done, all information about the contract is saved in digital certificates that can be used in the future. This function provides right information over time so that it builds market trust in society over time. Stored information and enhanced trust in the society can result in the increase volume and quality of service in the e-market.

III. STRUCTURAL DIAGRAM OF IPMP PROTOTYPE

In this section, the design of an IPMP model is illustrated in terms of structural diagram. Figure 1 shows the structural diagram for this IPMP e-commerce model. The system is built on a digital commerce market structure where a protected digital asset is exchanged through the Internet. The structural diagram gives a relationship between the key elements of IPMP infrastructure consisted of content suppliers (creator, rights-holder, etc.) and content users, DOI registration agency, data (and financial) clearing center, and Internet content service providers. Internet content service providers are consisted of four essential elements as content database, membership database, plug-in, and the IPMP engine in shown Figure 1.

Figure 1 Structural Diagram of IPMP



The system elements for the IPMP market differ from the current e-commerce market in three distinctive ways. First, all digital assets (and thereof their transactions) are identified and registered in DOI mechanism[17][18]. Second, digital assets and contents transactions are secured through encryption mechanism in the IPMP market. Third, all the transaction records are kept for later uses, which is through the internet data center (IDC). In these transaction processes, right management information (RMI), like digital resume for each product, is created for and attached to each digital or non-digital goods.

Detailed description for each element in the structural diagram in Figure 1 is shown as follows.

- Creator is a person (i.e., author) or an organization that create a digital asset.
- Rights-holder is a person or an organization that has rights over the digital asset existed. In reality, rights-holders and creators for the digital item may not be the same persons.
- Information (content) Provider (IP) is a person/organization that receives the digital asset from a creator, collects all information about the content, and produces the metadata model for it.

- Internet Service Provider (ISP) is a service provider through which all transactions are occurred. The role of ISP is to sale the digital asset received from IP. In this process, the sale information about a particular transaction is generated, and they are attached to the digital asset.
- Customer is a user who purchases the digital asset. The customer can copy, print, view, or play the purchased digital asset according to the options he purchased.
- Digital Object Identification Registration Agency (DOI RA) system here is denoted a unique object identifier for all digital objects.
- Internet Data Center (IDC) is an organization or mechanism where an actual transaction of all information is recorded and stored permanently.

Following gives the detailed implementation of IPMP prototype, focusing on encryption, content metadata, and structural diagram to capture right information that can be generated in the process of transaction events.

IV. Implementation of IPMP Relationship Prototype

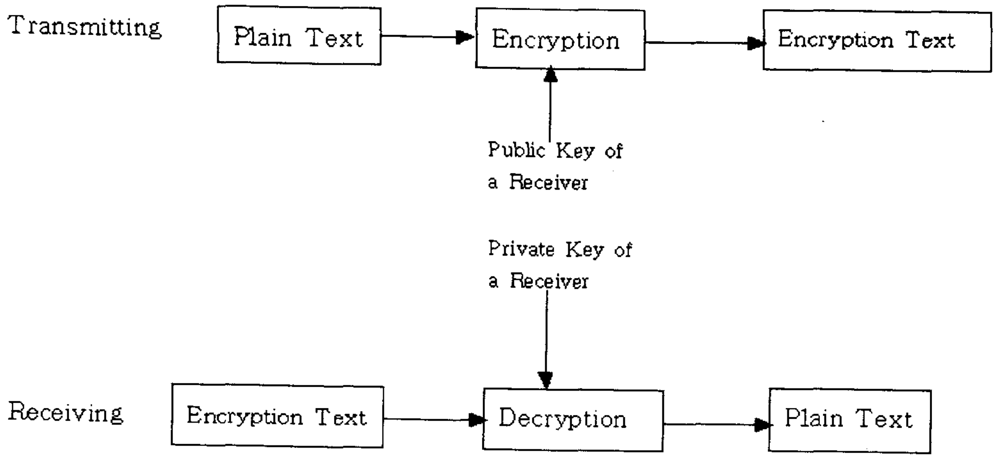
This section illustrates the implementation of the IMPM prototype build for a new e-commerce market. The actual coding has been done using a judicious mix of Java, Jsp, and XrML. XrML is used as a right language that specifies rights and issuing conditions of asset transactions[19][20]. To achieve safe protection and proper delivery of digital assets, three mechanisms are important: encryption algorithms, content metadata, and digital work itself captured in right language. Here we use XrML as denoted above.

4.1 Encryption Algorithms

In Internet environment, it is essential that some data transmitted between Web application processes is confidential. Among many methods that achieve confidentiality in data transmission, encryption method is the most basic and fundamental. For this reason, we discuss the Rivest, Shamir, and Adleman (RSA) algorithm, the popular cryptographic method illustrated in Figure 2.

Often, Internet users want to encrypt their message to protect their private information and rights. In the receiving end, the user needs to apply a reverse function, called decryption, to recover the original digital contents as shown in Figure 2

Figure 2 Encryption and Decryption Processes in the Internet



The RSA is an asymmetric key (public-key) cryptography. It uses a one-way mathematical function in that it is relatively easy to compute a result given some input values, but the reverse is extremely difficult. The RSA system uses modular arithmetic and elementary number theory. Specifically, the RSA algorithm has three steps: key generation, encryption (public key), and decryption (private key) as explained below.

(1) Key generation is to generate a public and private key by choosing two large prime numbers, p and q, and by multiply them together to get n.

(2) Encryption key (e) is an integer between 3 and n−1 satisfying gcd (e, λ(n)) =1, where λ(n)) = lcm (p−1, q−1).

(3) Decryption key (d) : in which the ciphertext C is raised to the power d, and then reduced modulo n.

Table 1 Algorithms of RSA system

Operation	RSA System
Encryption	$C = M^e \bmod n$
Decryption	$M = C^d \bmod n$
Modulus	Prime numbers, p, q
Encryption exponent (e)	E relatively prime to (p-1) * (q-1)
Decryption exponent (d)	$D = e^{-1} \bmod (p-1) * (q-1)$

While encryption method such as RSA algorithm may provide safety on transmission, digital or non-digital goods are needed to identify themselves at the spot as well as in the transaction processes. The following section gives how to identify digital items in e-commerce environment. Also rights information about digital asset should be also supplement along the process.

4.2 Asset Metadata

In e-market, a digital asset must be identified, described, and captured by some standard formats such as MPEG. Such standardization provides interoperability across the different platforms and technical infrastructure. Note that these content metadata are created before any transaction activity occurs. In other words, these information about the digital asset itself should be kept in separate data storage places from the transactional databases. Most information about digital asset is being created and captured during the transactional process. Following is an example of the XrML codes for Asset Metadata. Description of a particular transaction, along with brief content information, ownership and/or rights information, usage information, etc. would be contained in XrML Tags below.

```
〈XrML〉
〈BODY type="Kent Sample Data" version="1.0"〉
  〈ISSUED〉2000-4-30〈/ISSUED〉
       〈TIME〉
         〈FROM〉2000-04-30T00:00〈/FROM〉
                              〈UNTIL〉2050-08-
31T23:59:59〈/UNTIL〉
       〈/TIME〉
  〈DESCRIPTOR〉
       〈OBJECT type="Person"〉
         〈ID type="SSN"〉011-337-1234  〈/ID〉
       〈NAME〉David Brown〈/NAME〉
       〈/OBJECT〉
  〈/DESCRIPTOR〉
〈/BODY〉
〈/XrML〉
```

4.3 XrML

XrML (eXtensible rights Markup Language) provides a universal tool for specification of rights, fees, and issuing conditions (licenses) associated with the use and protection of digital asset. Based on the pioneering research from Xerox' Palo Alto Research Center (PARC), ContentGuard has developed XrML to unify the Intellectual Property Management and Protection (IPMP) specifications and encourage interoperability.

XrML facilitates the creation of an open architecture for rights management of digital asset and can be easily integrated with both existing and new systems. Specifically, XrML will enable users to:

- Describe rights, fees and conditions appropriate to commerce models they select.
- Provide standard terms for usage rights with useful, concise and easily understandable meanings.

- Offer vendors operational definitions of trusted systems for compliance testing and evaluation.
- Provide extensibility to new language features without compromising XrML's other goals.

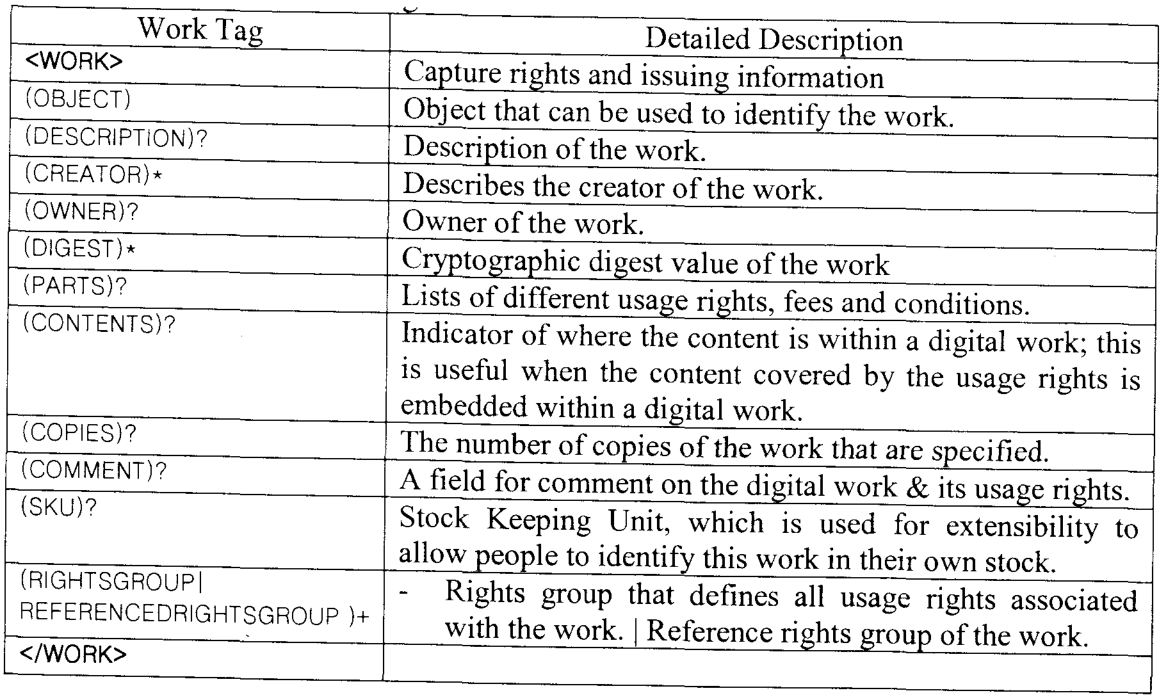
The use of XrML for usage rights on digital assets is to ensure that a IPMP framework provides trust and interoperability.

IPMP WORK Tag

XrML WORK Tags specify a digital work and its usage rights. The overall structure for defining the WORK is shown in Table 2.

Following is an example of XrML specification used in Movie called The Mummy, and its rights information and issuing conditions (OBJECT, DESCRIPTION, CREATER, OWNER, COMMENT, RIGHTGROUP, etc) are detailed in each XrML structural diagram below. Specially, this example gives two RIGHTGROUP information, home or theater. Depending on home or theater usage specification, different rights information (i.e, fee, copyright) is provided.

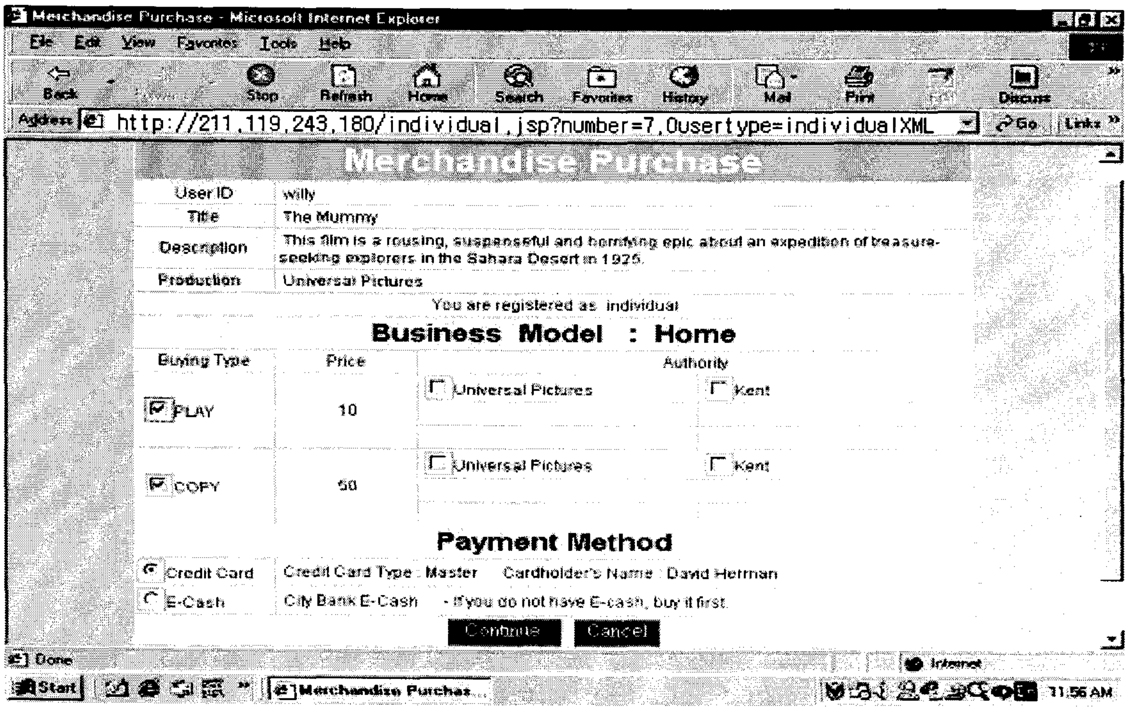
Table 2 Structure of Work Tag



Work Tag	Detailed Description
<WORK>	Capture rights and issuing information
(OBJECT)	Object that can be used to identify the work.
(DESCRIPTION)?	Description of the work.
(CREATOR)*	Describes the creator of the work.
(OWNER)?	Owner of the work.
(DIGEST)*	Cryptographic digest value of the work
(PARTS)?	Lists of different usage rights, fees and conditions.
(CONTENTS)?	Indicator of where the content is within a digital work; this is useful when the content covered by the usage rights is embedded within a digital work.
(COPIES)?	The number of copies of the work that are specified.
(COMMENT)?	A field for comment on the digital work & its usage rights.
(SKU)?	Stock Keeping Unit, which is used for extensibility to allow people to identify this work in their own stock.
(RIGHTSGROUP| REFERENCEDRIGHTSGROUP)+	- Rights group that defines all usage rights associated with the work. | Reference rights group of the work.
</WORK>	

```
〈WORK〉
        〈OBJECT type="film" version="1.0"〉
          〈ID type="DOI"〉10.1131/2000/video7〈/ID〉
          〈NAME〉The Mummy 〈/NAME〉
        〈/OBJECT〉
        〈DESCRIPTION〉 This film is a rousing, suspenseful and horrifying epic about an expedition of
                                treasure-seeking explorers in the Sahara Desert in  1925.
           〈/DESCRIPTION〉
        〈CREATOR type="Director"〉 Stephen Sommers 〈/CREATOR〉
        〈OWNER〉〉
          〈OBJECT type="Corporation"〉
           〈ID type="registration number"〉ROK-8234045〈/ID〉
            〈NAME〉Universial Pictures〈/NAME〉
            〈ADDRESS type="Postal"〉"〉 P.O.Box 8152 Universal City, CA91618-8152〈/ADDRESS〉
            〈ADDRESS type="URL"〉www.universalstudio.com〈/ADDRESS〉
          〈/OBJECT〉
        〈/OWNER〉
        〈COMMENT〉This content is hypothetical so that it may not be real.〈/COMMENT〉



        〈RIGHTSGROUP name="Home"〉
          〈COMMENT〉This is for a home use.〈/COMMENT〉
          〈BUNDLE〉
                〈ACCESS〉
                  〈PRINCIPAL type="user"〉
                        〈ENABLINGBITS type="sealed-private-key"〉
                          〈VALUE encoding="base64" size="64"〉dsfjkl33423=〈/VALUE〉
                        〈/ENABLINGBITS〉
                        〈CERTIFICATE〉
                          〈AUTHORITY id="Universal Pictures"〉〈/AUTHORITY〉
                          〈PROPERTYPAIR name="type" value="Distributor" /〉
                        〈/CERTIFICATE〉
                  〈/PRINCIPAL〉
                〈/ACCESS〉
                〈FEE〉 〈TICKET type="Pre-paid"〉
                        〈AUTHORITY id="Kent" /〉〈/TICKET〉〈/FEE〉
                〈FEE〉〈MONETARY〉
                        〈ACCOUNT〉〈ACCOUNTTO id="213-43-455"/〉
                          〈HOUSE id="City Bank" url="www.citybankonline.com"/〉
                        〈/ACCOUNT〉〈/MONETARY〉 〈/FEE〉

                〈TERRITORY〉
                  〈LOCATION country="USA" /〉
                〈/TERRITORY〉
          〈/BUNDLE〉
          〈RIGHTSLIST〉
          〈COPY〉
                  〈NEXTRIGHTS〉
                        〈RIGHTSTODELETE name="Theater"/〉〈/NEXTRIGHTS〉
                        〈CERTIFICATE〉
                                〈AUTHORITY id="Kent"〉 〈/AUTHORITY〉
                        〈/CERTIFICATE〉
                  〈FEE〉〈MONETARY〉〈PERUSE value="50"/〉〈/MONETARY〉 〈/FEE〉〈/COPY〉
                〈PLAY〉
                  〈PLAYER〉〈CERTIFICATE〉
                        〈AUTHORITY id="Kent"〉〈/AUTHORITY〉
                        〈PROPERTYPAIR name="Class" value="Video-player"/〉
                          〈/CERTIFICATE〉 〈/PLAYER〉
            〈FEE〉〈MONETARY〉 〈PERUSE value="10"/〉〈/MONETARY〉〈/FEE〉
        〈/PLAY〉

    〈/RIGHTSLIST〉
  〈/RIGHTSGROUP〉
〈/WORK〉
```

Figure 3. Screen Shot of Implementation of IPMP prototype


Merchandise Purchase - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address
Go Links
Done
Internet
Start
Merchandise Purchas...
11:56 AM

http://211.119.243.180/individual.jsp?number=7,0usertype=individualXML

Merchandise Purchase

User ID	willy
Title	The Mummy
Description	This film is a rousing, suspenseful and horrifying epic about an expedition of treasure-seeking explorers in the Sahara Desert in 1925.
Production	Universal Pictures

You are registered as individual

Business Model : Home

Buying Type	Price	Authority	
☑ PLAY	10	☐ Universal Pictures	☐ Kent
☑ COPY	50	☐ Universal Pictures	☐ Kent

Payment Method

● Credit Card	Credit Card Type : Master Cardholder's Name : David Herman
○ E-Cash	City Bank E-Cash - If you do not have E-cash, buy it first.

Continue Cancel

Figure 3 gives a screen shot of the implementation of IPMP prototype that shows three sub sections: merchandise purchase, business model (home or office, in this study), and payment method. As one can see, this IPMP prototype provides not only the basic e-commerce information such as shown in merchandise and payment method sections but also the right property information (i.e., how many options are available associated with a purchase?). In this particular case, two options, play and copy functions, are award to the home user. Of course, such information is transmitted through encryption methods such as RSA algorithms used in this study. Thus, intellectual property management and protection effort provides reliable and trustworthy environment by utilizing Internet and network security measures such as encryption, watermarking, digital certificates as well as better service business surrounding by giving the tailor made transaction for each of market participants, customers, right holders, and retailers for their needs. Thus, IPMP market mechanism may significantly enhance the volume and quality of e-commerce and digital economy.

V. FUTURE RESEARCH/CONCLUSION

In 21 Century, intellectual creativity and property of human capital has recognized the most valuable resource. IPMP technologies are designed to protect intellectual property (IP) of the user. In this study, we identify the deficiency of the current version of e-commerce and try to provide rights information by building the IPMP-based commerce model to supplement the current e-commerce service.

We first provide the structural diagram for the prototype of a Intellectual Property Management and Protection and then implement the prototype using XrML, JSP, and encryption algorithms, and Java. We explain right information description especially by illustrating the details of XrML Work tags.

In sum, digital information is now predominant forms of data traffic and data description format in this digital age. For such environment, management and protection for rights information on digital or non-digital items is getting important. Thus IPMP mechanism would provide the current e-market with trust and safety measures to secure electronic transaction and quality of service.

References

1. Neylon, E., " First Steps In An Information Commerce Economy : Digital Rights Management In The Emerging Ebook Environment," D-Lib magazine, Vol. 7, No. 1, January 2001, Vol. 7, No. 1, ISSN 1081-9873.
2. World Intellectual Property Organization, [http://www.wipo.org]
3. Iannella, R., " Digital Rights Management(DRM) Architectures," D-Lib Magazine, June 2001, Vol7, No.6, [www.dlib.org/dlib/june01/iannella/06iannella.html]
4. Park, P., Sandhu, R., and Schifalacqua, J., "Security Architecture for Controlled Digital Information Dissemination," The Proc. of Annual Computer Security Applications Conference (ACSAC), New Orleans, Louisiana, Dec. 2000. [dilb.computer.org/conference/acsac/0859/pdf/08590224.pdf]
5. Rue, D., "Digital Watermarking for rights protection for movies," Journal of multimedia association, vol. 2, no. 4, 1999.12. pp. 438-450
6. Bailey, D.V., "Inside eBook Security," Dr. Dobb' s Jounral Nov. 2001, [http://www.ddj.com/]
7. Davis, T.M. and Lafferty, Tim., "Digital Rights Management: Implications for Libraries," The Bottom Line: Managing Library Finances, Vol. 15, No. 1, 2002, pp. 18-21.
8. Erickson(a), J.S. "A Digital Object Approach to Interoperable Rights Management," D-Lib Magazine, June 2001, Vol. 7, No. 6., ISSN 1082-9873 [http://www.dlib.org/dlib/june01/erickson/06erickson.html]
9. Torrubia, A., J.Mora, F., and Marti, L., "Cryptography Regulations for E-commerce and Digital Rights Management, Computer & Security, vol 20, no. 8, 2001, pp 724-738.
10. Moving Pictures Experts Group, [http://www.self.it/mpeg]
11. Koenen, R., "Intellectual property management and protection in MPEG," [http://www.mpeg.org]
12. Erickson(b), J.S. "Information Objects and Rights Management," D-Lib Magazine, April 2001, Vol. 7, No. 4., ISSN 1082-9873, [http://www.dlib.org/dlib/april01/erickson/04erickson.html]
13. Mooney, S., "Interoperability: digi-tal rights management and the emer-ging ebook environment," D-Lib Magazine, January 2001, Vol. 7, No. 1, ISSN 1082-9873. 1-6, [http://www.dlib.org/dlib/january01/mooney/01mooney.html]
14. AAP: Association of American Publisher [http://www.publishers.org]

* 15. Chi-Wei Yang, Paul C. H. Lee, Ruei-Chuan Chang, "Content-Based Digital Signature for Motion Pictures

Authentication and Content-Fragile Watermarking," IEEE International Conference On Multimedia Computing and Systems, 1999, Vol.2, pp 209-213

*16. Deepa Kundur Dimitrios Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication," Proceedings of The IEEE, July 1999, Vol. 87, No. 7, pp 1167-1180

17. Norman Paskin, The DOI Handbook, version 0.3 July, 2000

18. Norman Paskin, "2000, The Digital Object Identifier Initiative: Current Position and Review Forward," IDF, [http://www.doi.org]

19. XrML: eXtensible rights Markup Language, [http://www.XrML.org]

20. Digital Property Rights Language, [http://www.coverpages.org/DPRLmanual-XML2.html]