A Novel Approach to Digital Contents Sharing for Digital Home Network

[1]Danmei Niu, [2]Zhiyong Zhang, [3]Shaofeng Wang, [4]Lili Zhang
[1,2,4]*Electronic Information Engineering College, Henan University of Science and Technology, Luoyang, China, niudanmei@163.com, z.zhang@ieee.org, lillyzh@126.com*
[3]*The Electricity Examination Department, The Patent Office of SIPO, P.R.C, Beijing, China, wangshaofeng@sipo.gov.cn*

Abstract

The purpose of Digital Rights Management (DRM) is to prevent the illegal copying and distribution of digital contents. Common DRM, however, is inappropriate for a digital home environment that consists of family members and devices. Different family members need different access rights to DRM contents in their home networks. This paper presents a novel approach to digital contents sharing for digital home network. This approach adopts the idea of Role-Based Access Control (RBAC) and license chain and allows digital contents sharing to be convenient and controlled. Through analyzing the performance of the approach, we conclude that this novel approach is more secure and flexible, and it satisfies the requirement of digital home networks.

Keywords*: Digital Rights Management, Home Network, Contents Sharing, Role-based Access Control*

1. Introduction

The development of the network has made distributing digital multimedia contents easier. The digital content provides conveniences such as ease in copying, allowing the copied content to be identical to the original. Such a convenience, however, involves illegal activities like copyright piracy and illegal copying [1].

Recently, Digital Rights Management (DRM) has been used for preventing illegal copying and distribution without the allowance of the copyright owners [2-4]. DRM allows the copyright owners to control and monitor the distribution of the digital contents through electronic channels using a machine enforceable license, and it has become a fast-growing field of research and development in recent years. A number of related systems are now commercially available [5-8].

Networking is rapidly being adopted in the home. Multiple computers can share a broadband connection via either a wired or wireless network, and there are an increasing number of digital devices in a home network. From the family user's point of view, the user wants to play and transfer the digital contents freely on any of his multiple devices and realize the uniform management. Common DRM is appropriate to general network environment but inappropriate to the digital home environment. The concept of Authorized Domain (AD) has been presented to resolve such problems [9, 10]. Each device has equivalent access rights on the digital contents, only if it is registered in home network. However, certain contents such as adult contents, which are not allowed to children, are to be managed with access control [11]. That is, in a home network, different users should have different rights.

In this paper, we present a novel approach to digital contents sharing for digital home network. The approach is based on Role-Based Access Control (RBAC) and license chain that controls the access rights of family members and devices.

The remainder of this paper is organized as follows: in Section 2, we investigate the background and motivation. The classification of roles and distribution of permissions for the home network are explained in detail in Section 3. Section 4 shows a DRM functional architecture for the home network and the form of the licenses, and explains the structure of license chain and the working process. In Section 5, we analyze the performance and security and make a comparison of three approaches. Section 6 concludes the paper.

2. Background and motivation

Figure 1 depicts a typical real home network. Home network is the major applied form of AD. Note that it includes a mix of wireless and wired connectivity, along with a range of devices, including PCs, printers, smartphones, cameras, etc [12].

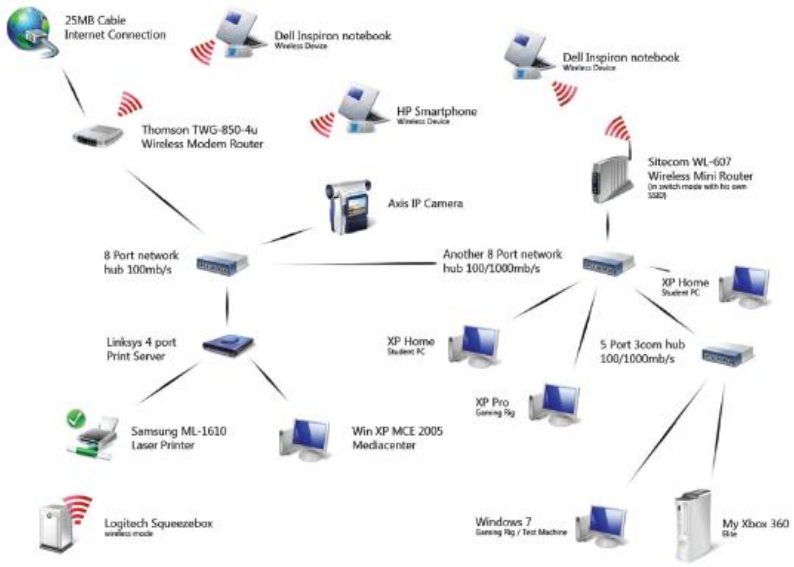

Figure 1. A typical real home network

There are several ways of allowing differentiation for rights within a domain [13-16]. A straightforward solution would be to introduce differentiations during the purchase of the rights when the user could immediately define different rights for different domain members and let content provider encode this in the licenses. However, this is a rather static, non-flexible, and privacy invasive approach.

Furthermore, introduce differentiations in the process of transcoding delivery DRM rights into domain DRM rights. Here, a person who bought the content (or, domain administrator or a domain member who first accesses the license) will be allowed to add further restrictions or rights on top of the original rights, which are used to control the use of and access to content in a domain. However, a very strong requirement by the commercial content providers is an ability to completely control the content distribution and usage. Very often, content providers neither trust nor allow transcoding of original licenses.

Another possibility is letting the domain administrator adds a chain for every license distributed to the domain. The chain records devices information of playing DRM contents. This approach realizes tracing of a license in a domain and does not change the original license. However, this cannot provide appropriate rights to each member and device in a domain.

In a digital home network, if a user buys digital contents, other users in the home network may be allowed to access that content as well. This causes a number of privacy and security problems. In some certain scenes, because of parental control, privacy, individual interests and so on, the domain administrator does not wish other users of the domain to use certain digital contents. For example, in order to prevent children from spending too much time on the digital contents, parents do not allow children to view some adult contents, or they only agree to children playing the digital contents within a limited time to prevent overuse. Another example is if you only wish to share some contents, such as music or movies, with a friend joining your home network with his device. Therefore, in order to remove these potential security and privacy problems, we present a novel approach that controls the access rights of each family member.

3. Classification of roles and distribution of permissions for home network

3.1. RBAC model

The novel approach is based on RBAC. The core idea of RBAC is creating relations between permissions and roles and distributing appropriate roles to users. Then users can have relations with permissions [17]. Setting up roles is based on different tasks, and distributing roles to users is based on users' responsibility. An example of a famous model is RBAC96 [18]. Figure 2 illustrates the model.

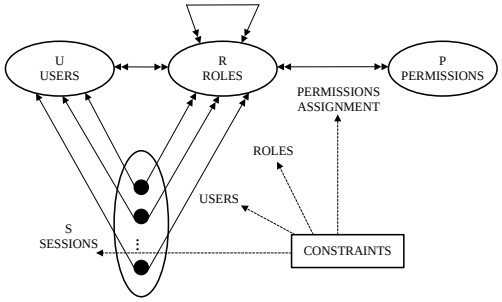

Figure 2. RBAC model

There are three sets of entities called users (U), roles (R), and permissions (P). Figure 2 also shows a collection of sessions (S). A user is the operational main body of data objects, and in this model it is a human being.

Role is a job function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role. Roles act as middle bridges that link users and permissions.

Permission is an approval of a particular mode of access to one or more objects in the system. The terms authorization, access right and privilege are also used to denote permission. Permissions are always positive and confer the ability to the holder of the permission to perform some actions in the system.

Constraint appends each element of RBAC model and is used to express the condition of permission.

Session is an active concept. Sessions are created when users activate roles.

3.2. Classification of roles for home network

According to the responsibilities and requirements of different users in a home network, we classify the roles and design a model of role hierarchies for the home network. Figure 3 shows this model.

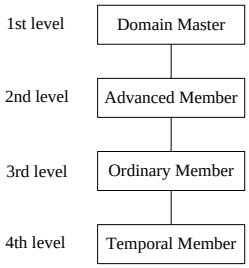

Figure 3. A model of role hierarchies

Role hierarchies are natural means for structuring roles to reflect an organization's lines of authority and responsibility. By convention, more powerful or senior roles are shown toward the top, and less powerful or junior roles are shown toward the bottom.

In this model, there are four levels. The fourth level is the junior-most level, and the temporary member is in this level. In most cases, this is a user who temporarily shares digital contents with the users of the home network. Or, the temporary member has partial permissions of using DRM contents and has the lowest permission.

Ordinary member is in the third level. This member is senior to the temporary member and thereby inherits all permissions from the temporary member. The ordinary member can have permissions in addition to those inherited from the temporary member. The permission of this role includes requesting and using DRM contents or licenses, but it has some limitations. For example, children can be the users of this role and only play some DRM contents within some time of the day (for example, 8:00-21:00).

Inheritance of permissions is transitive. In Figure 3, the advanced member is in the second level. This role inherits permissions from the both ordinary member and temporal member. Advanced member can have additional permissions. For example, the adults or parents of a family can be distributed this role and possess most of permissions.

Domain master is in the first level. Only one family member can be the domain master who is the owner or administrator of a home network domain. Domain master is the principal and the highest manager. This role inherits permissions from advanced member, ordinary member and temporal member. Domain master has all the permissions.

3.3. Distribution of permissions for home network

Role is an intermediary between a user and permissions. By distributing a role to a user and then distributing permissions to the role, the user can then obtain the corresponding permissions. There are many permission types for the home network, such as creating and deleting domain, adding and deleting users or devices, etc.

According to the above mentioned roles, family members can act as these roles and then have different permissions. For example, a father or mother can act as domain master who has all the permissions. Their children can act as ordinary members and have less permission, and some contents and devices are limited to use during a specific time per day. A friend who is joining the home network temporarily can act as temporary member who can only share movie or music with other family members. So, we need to distribute appropriate permissions to the four kinds of roles. We create a table of relations for users, roles and permissions in Table 1.

Table 1. A table of relations for users, roles and permissions

Users	Roles	Permissions
Family member 1 Family member 2 … Family member n	Domain master	Creating/deleting/updating domain Adding/deleting users/devices Setting up maximal number of users/devices Requesting for joining/leaving domain Purchasing DRM contents Requesting/using DRM contents Requesting/using licenses Managing/distributing DRM contents and licenses
	Advanced member	Requesting for joining/leaving domain Purchasing DRM contents Requesting/using DRM contents Requesting/using licenses Managing DRM contents and licenses
	Ordinary member	Requesting for joining/leaving domain Requesting/using DRM contents Requesting/using licenses
	Temporal member	Requesting for joining/leaving domain(temporarily) Requesting/using DRM contents(limited) Requesting/using licenses(limited)

This table is managed dynamically by the domain master. When a family member registers or leaves the domain, or his role changes, the domain master dynamically determines the permissions of the role for the user.

4. A novel approach to digital contents sharing for digital home network

In this section, we propose a novel approach to digital contents sharing for digital home network based on RBAC. We adopt the license chain in the approach. The chain is used for tracing license, and recording information of family members and devices.

4.1. A DRM functional architecture for home network

In Figure 4, we design a DRM functional architecture for home network.

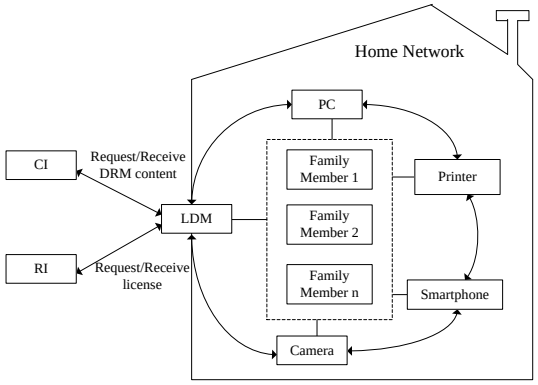

Figure 4. A DRM functional architecture for home network

The architecture consists of the following functional entities:

CI (Content Issuer): CI has the responsibility for providing digital contents issuing and downloading. The digital contents which are requested by the user are packed and encrypted by CI (the encrypted contents are called DRM contents). Then, CI sends DRM contents to the legal home network. CI also communicates with RI and allows RI to create corresponding licenses.

RI (Rights Issuer): RI has a responsibility for creating and distributing corresponding licenses of DRM contents. According to the received information from CI, RI creates corresponding licenses and then distributes the licenses to the legal home network.

LDM (Local Domain Manager): LDM is the core device of a home network. It stores the list of all the family members and devices of a home network with the responsibility for managing them. LDM administers the registration of the family members and devices, confirming the identity and permissions of the family members. The table of relations for users, roles and permissions is stored in LDM. It requests DRM contents and corresponding licenses from CI and RI, and then it distributes the acquired DRM contents and licenses to the family members and devices. LDM does not need to be a special device; it can be a PC or a notebook PC. It should, however, have enough memory space, working capability and high security. There is only one LDM in a home network.

Devices such as the PC, printer, smartphone and camera are connected in a home network, and the home network can be wired or wireless. In this system, all the devices are trusted and posses certificates issued by Certificate Authority (CA). Each device has a public key and a private key. Devices access DRM contents through local or remote access approach and display the description of the domain according to the family members who are using them.

Family members are the users of the devices and must register in the domain. They can share several devices and display DRM contents on the devices.

4.2. License description

When a family member pays the content provider for DRM contents, CI transfers DRM contents to LDM. The contents should also be played in other devices that are members of the home network. To support this capability, RI transfers licenses for the purchased contents, which is only accessible to LDM.

The license form follows ITUTX.509 international standard. In this paper, the form of the license is shown in Figure 5.

License information: version number, serial number, signature algorithm;
License owner information: identity, public key;
Content information: ID, decryption key;
Using permissions: using constraints of content, valid term;
Digital signature of RI.

Figure 5. The form of the license

License information includes version number, serial number (a unique number for each license), and a signature algorithm (such as RSA algorithm). License owner information includes an identity and a public key. Content information includes ID and a decryption key used to decrypt DRM content. Using permissions includes using constraints of contents, and there are several types of constraints such as using times of DRM contents, number of devices using the DRM contents at the same time, valid term, etc. The UTC time form is used for valid term. The digital signature of RI is included in the license, assuring integrity. Once the license is purchased, it cannot be modified.

License could be described with Rights Expression Language (REL). REL is an important part in the DRM research area, which is used to describe the user rights of digital contents or services. REL could describe the user rights of a party who owns some assets. Right, asset and party are basic entities of REL. Right means using or accessing permission of asset, which includes permission, prerequisite condition and restrictive condition, etc. Asset is a digital content or service with a unique identity. Party is a corporation entity or individual related with the resource, including the copyright owner, author, content provider and user.

REL must be convenient and easy to use. It should be open, flexible and expansible. REL could describe a variety of user rights of DRM contents. Extensible rights Markup Language (XrML) and Open Digital Rights Language (ODRL) are two mature rights expression languages based on Extensible Markup Language (XML), which have been adopted by some standard organizations.

4.3. Structure of license chain

In this paper, we add a chain for each license. The chain is used for recording the information of the devices and family members using DRM contents. The chain is managed by LDM and only used in the home network. Current device and family member using the digital content is identified in the chain, which assures the license only on one device used by one family member at the same time. Once the license is transferred to other users and devices, the original family member and device cannot use this license to play the corresponding digital content anymore. This approach constrains some permission, such as play times and term and is more flexible. The structure of chain is shown below:

Record 1: Content ID，
Sender (family member ID1, device ID1),
Receiver (family member ID1', device ID1'),
Timestamp 1,
Digital signature of family member ID1.
Record 2: …
Record n: Content ID，
Sender (family member IDn, device IDn),
Receiver (family member IDn', device IDn'),
Timestamp n,
Digital signature of family member IDn.
Current device n

There are several records in a chain, which includes content ID, sender information, receiver information, timestamp and digital signature of family member IDn.

4.4. Working process

The working process of the approach is shown below:

Firstly, when a family member in the home network requests the digital content and the corresponding license, he or she let LDM request and receive the content and license from RI and CI.

Then, the family member sends LDM a message, including family member ID, device ID and requested content ID. LDM checks if the family member and the device are legal and then queries the table of relations for users, roles and permissions. According to the table, LDM decides if the family member has the using permission for the digital content.

If the family member has the using permission, LDM sends the encrypted content to the device which the family member is using. The encrypted content can be stored in any device and can be transferred freely in the home network.

Suppose there is an information table of using licenses in LDM, which records the corresponding licenses of DRM contents. This table includes the current family member ID and device ID using DRM contents, and the serial number of corresponding licenses. The domain master will check the table in LDM. If the license is in LDM, the domain master will write a record in the chain and will then encrypts the license and the attached chain with the public key of receiving device. He will also send them to the device used by the family member. It is necessary for LDM to record the serial number of the license, family member ID and device ID in the information table of using the license.

If the license is not in LDM, the domain master will check the information table of using the license. Then, he can find out the current family member ID and device ID using the digital content and then send a message to them. The family member who is using the license writes a record in the corresponding chain and then encrypts the license and the attached chain with the public key of receiving device. He sends them to the receiver, and the sender cannot play that content anymore. The sender should also send the receiver information to LDM. The information table of using license is updated by the domain master.

When the family member obtains the license, he should decrypt the license and the attached chain with the private key of the receiving device and then get the decryption key. The family member can decrypt the digital content with the decryption key and play the content. If the decrypted content is terminated, it should be deleted immediately. All devices are forbidden to store and copy the decrypted content.

When the permission of a license is used up – that is, the using times of the content becomes 0, or the valid term expires – the last family member who is using the license sends the license and the attached chain to LDM. The domain master will conduct a statistical analysis according to the license and the chain.

5. Analysis and comparison

5.1. Analysis of performance and security

This novel approach is based on RBAC and the license chain. All the family members can share DRM contents according to the corresponding permissions of their roles. The performance of the approach is analyzed below:

The concept of AD has been adopted in the home network, and the licenses of DRM contents are bound with a group of devices, not one device. The encrypted digital content can be stored in any device and be transferred freely in the home network. The communication among RI, CI and the devices of home network is simplified greatly. The amount of issuing licenses and DRM contents, and the cost of resources are reduced greatly. The burdens of RI and CI are decreased.

The combination of RBAC and license chain is used in this approach, which realizes tracing license and transferring permission. It is convenient for the domain master to manage DRM contents and the licenses. Meanwhile, the domain master can make a statistical analysis according to the licenses and chains.

Every family member and device would have the most appropriate permission based on the table of relations for users, roles and permissions. The control over the differentiation for rights is more flexible, because content provider can control the content distribution and usage in home network without encoding additional information in the licenses.

The following is the analysis of security:

Our novel approach adopts the DRM architecture. DRM contents are separated from the licenses, which increases the flexibility of management. If DRM contents are modified, the corresponding issued licenses are not influenced. The security is also improved. Even if an illegal user gets DRM contents, he or she does not have the licenses and cannot decrypt DRM contents. This method prevents illegal access.

In the working process of the approach, when a family member wants the digital content and the corresponding license, LDM will check if the family member ID and the device ID are legal. This working method can identify the illegal users and devices and prevent illegal users from playing the digital content in unauthorized devices.

In a home network, the sender should encrypt the license and the attached chain with the public key of the receiving device. The receiver will decrypt the license and chain with the private key of receiving device and then get the decryption key of the digital content. In this way, except for the sender and receiver, the license cannot be taken by others. This method also assures no modification during the transferring of the license, which is real and reliable.

At one time, only one family member can play the digital content on one device. Every time the decrypted content is used up, it should be deleted immediately. Any device is forbidden to store and copy the decrypted contents, which prevents arbitrary copying.

5.2. Comparison of approaches

There are two main approaches of license management within the domain now. One is introducing differentiations during purchase of the licenses, and the other is introducing the domain administrator or a domain member who first accesses the license creating the domain licenses. We can make a comparison of these two approaches and our novel approach in Table 2.

Table 2. Comparison results of three approaches

Approaches	Security	Complexity	Flexibility	Disclosing privacy	Changing licenses
Purchasing different licenses	High	High	Low	Yes	No
Creating domain licenses	High	High	High	No	Yes
Novel approach	High	Low	High	No	No

Regarding the security of digital contents management, DRM architecture is adopted in the three approaches which can prevent from the illegal copying and distribution. DRM contents can be used only with the decryption key. If the digital content is used up, it should be deleted immediately. The security performance of all the approaches is high.

The purchasing different licenses approach is letting content provider encode differentiations in the licenses, so the communication traffic and workload between the content provider and the domain member increases. This approach is complex. In creating domain licenses approach, the domain administrator or a domain member who first accesses the licenses will be allowed to add further restrictions on top of the original licenses, and then distributes these domain licenses to other domain members. Because of this, the burden of domain administrator or domain members is high, and the complexity of this approach is high, too. Our novel approach adopts the license chain to trace license, and the RBAC model is used. We have utilized unified and effective management, and the complexity performance is low.

Purchasing different licenses approach is not flexible. When a domain member needs DRM contents, he should get a new license from the content provider. The other two approaches are flexible, as the domain administrator manages the distribution of DRM contents and licenses effectively.

It is easy to disclose the privacy of domain members in the purchasing different licenses approach, but the other approaches are not easily disclosed.

Purchasing different licenses and our novel approach reserve the structure and function of the original licenses, but the creating domain licenses approach will change the license form.

According to the above-mentioned comparison, we can see that our novel approach possesses the advantages and overcomes the disadvantages of the other two approaches. Also, it realizes unified and

effective management of users and permissions. This novel approach is very suitable for digital contents sharing in the home network environment.

6. Conclusion and future work

In the typical DRM system, the licenses are bound with devices, which constrain the flexibility of using DRM contents. In this paper, we propose a novel approach to digital contents sharing for a digital home network. This approach is based on RBAC and license chain that controls the access rights of family members and devices. It satisfies the needs for family users. DRM contents can be transferred and used in home networks conveniently, quickly and freely.

Our future work will concentrate on how to realize the approach concretely and make the working process more efficient, etc.

7. Acknowledgment

We would like to express our gratitude to the anonymous reviewers of this paper for their helpful comments and suggestions. The work was sponsored by the National Natural Science Foundation of China (Grant No.61003234), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No.2011HASTIT015), China Postdoctoral Science Foundation (Grant No.20100471611), and Henan University of Science & Technology Doctors Research Fund (Grant No.09001470).

8. References

[1] Lesk M, Stytz MR, Trope RL, "Digital Rights Management and Individualized Pricing", IEEE Security & Privacy, vol. 6, no. 3, pp.76-79, 2008.
[2] Rosenblatt B, "DRM, Law and Technology: an American Perspective", Online Information Review, vol. 31, no. 1, pp.73-84, 2007.
[3] Lian S, "Secure Video Distribution Scheme Based on Partial Encryption", International Journal of Imaging Systems and Technology, vol. 19, no. 3, pp.227-235, 2009.
[4] Zhang ZY, Lian SG, Pei QQ, "Fuzzy Risk Assessments on Security Policies for Digital Rights Management", Neural Network World, vol. 20, no. 3, pp.265-284, 2010.
[5] Sheppard NP, Reihaneh SN, "Sharing Digital Rights with Domain Licensing", In Proceedings of the ACM International Workshop on Multimedia Contents protection and security, pp.3-12, 2006.
[6] Zhang ZY, Pei QQ, Yang L, "Game-Theoretic Analyses and Simulations of Adoptions of Security Policies for DRM in Contents Sharing Scenario", Intelligent Automation and Soft Computing, vol. 17, no. 2, pp.191-203, 2011.
[7] Wu CC, Lin CC, Chang CC, "Digital rights management for multimedia content over 3G mobile networks", Expert Systems with Applications, vol. 37, no. 10, pp.6787-6797, 2010.
[8] Zhang ZY, "Digital Rights Management Ecosystem and its Usage Controls: A Survey", International Journal of Digital Content Technology and its Applications, vol. 5, no. 3, pp.255-272, 2011.
[9] Feng X, Tang Z, Yu YY, "An Efficient Contents Sharing Method for DRM", In Proceedings of 2009 Consumer Communications and Networking Conference, pp.1-5, 2009.
[10] Lee TY, Lee HM, Chen WY, Chen HS, "Processing Logical Access Control Command in Computer System", International Journal of Digital Content Technology and its Applications, vol. 2, no. 2, pp.11-15, 2008.
[11] Kim H, Lee Y, Chung B, Yoon H, Lee J, Jung K, "Digital Rights Management with Right Delegation for Home Networks", In Proceedings of the 9th International Conference on Information Security and Cryptology, pp.233-245, 2006.
[12] Edwards WK, Grinter RE, Mahajan R, Wetherall D, "Advancing the State of Home Networking", Communications of the ACM, vol. 54, no. 6, pp.62-71, 2011.
[13] Lee J, Kim J, Park J, Yoon K, "Domain Based Content Sharing in Digital Home", In Proceedings of 2009 Fourth International Conference on Internet Monitoring and Protection, pp. 62-65, 2009.

[14] Petković M, Koster RP, "User-Attributed Rights in DRM", In Proceedings of Digital Rights Management: Technologies, Issues Challenges and Systems - First International Conference, pp.75-89, 2006.
[15] Lee S, Kim J, Hong SJ, "Redistributing Time-based Rights between Consumer Devices for Content Sharing in DRM System", International Journal of Information Security, vol. 8, no. 4, pp.263-273, 2009.
[16] Lee WB, Wu WJ, Chang CY, "A portable DRM scheme using smart cards", Journal of Organizational Computing and Electronic Commerce, vol. 17, no. 3, pp.247-258, 2007.
[17] Tsai DR, Chen WY, Liang CH, Hu CC, "Role-Based Access Control of Digital Right Management", In Proceedings of 2009 Fifth International Joint Conference on INC, IMS and IDC, pp.1131-1134, 2009.
[18] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE, "Role-Based Access Control Models", IEEE Computer, vol. 29, no. 2, pp.38-47, 1996.