DRM Cloud Architecture and Service Scenario for Content Protection*

Hyejoo Lee[1], Changho Seo[1], and Sang Uk Shin[2†]
[1] Kongju National University, ChungNam, Republic of Korea
hyejoo2010@gmail.com, chseo@kongju.ac.kr
[2] PuKyong National University, Busan, Republic of Korea
shinsu@pknu.ac.kr

Abstract

The smart devices and cloud computing technology have been introduced into a new content service such as N-Screen service. The DRM(digital rights management) techniques have been rapidly developed in accordance with the new service environment after the awareness on the importance of DRM technology. In spite of the technical advancement of DRM, it is being taken as an unwelcome thing by the content consumers until now. In the Cloud era, the rapid introduction of service is possible and also the importance of content protection is going to increase more and more. As a result, the DRM technology should be changed to match the nature of the Cloud as well. In this paper, a model of DRM-as-a-Service for content protection within the Cloud, which is referred to as DRM Cloud, and an architecture of DRM Cloud are proposed. Also we describe the content download service by using the DRM Cloud and discuss about the establishment of the trusted DRM Cloud and its advantages.

Keywords: Digital Rights Management, Cloud Computing, Content Protection, Interoperability

1 Introduction

With the development of smart devices and cloud computing technology, new service types have been introduced[1, 10, 14]. For example, there is N screen service that shares the digital contents through the integration of various smart devices. It assures QoS(quality of service) in a variety of network environments and provides the digital contents for a user who owns several devices such as TV, PC, and smart phone at the same time.

The DRM technologies have been advanced by adding new technologies to support multi-platforms and interoperability between DRMs for new content services[9, 13, 15]. Despite this development, still the content consumer does not purchase the DRM-protected contents without hesitation due to a discomfort or a negative awareness about the DRM technology. As a result, the content service providers, for example, Apple[2] become to provide DRM-free contents through a limited service such as streaming. Also the development costs are increasing because DRM developers or device manufacturers have to produce all sorts of DRM modules to support the content service. In addition, the content service providers want to provide the content consumers with various content service so as to keep the consumers they have and to subscribe new consumers to their service. Thus we propose the model of DRM-as-a-Service so that the content consumers use readily the DRM-protected contents, the content service providers provide the consumers with a variety of content service and the DRM developers can decrease the costs

Journal of Internet Services and Information Security (JISIS), volume: 3, number: 3/4, pp. 94-105

*This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Plannig (No.2011-0029927)

†Corresponding author: Room 1314, Building 1, Department of IT Convergence and Application Engineering, Daeyeon Campus (608-737) 45, Yongso-ro, Nam-Gu. Busan, Republic of Korea, Tel: +82-(0)516296249

of development. This model is referred to as the DRM Cloud. For this, the conception and architectural layers of the DRM Cloud are proposed and also the processes for content download service are described by using the DRM Cloud.

The organization of this paper is as follows. In section 2, the recent DRM technologies are introduced briefly. In section 3, the conceptual model of the DRM Cloud, the architectural layers and the service procedure for the content registration, the content download, and the domain management. In section 4, we discuss how to establish of trust DRM Cloud, the comparison of DRM technologies and the advantages of the DRM Cloud. In final section, further study is presented as a conclusion.

2 Related technologies

There are many of DRM technologies such as DECE(digital entertainment content ecosystem)'s UltraViolet ecosystem[11], Marlin DRM of MDC(Marlin Developer Community)[3], Microsoft's PlayReady ecosystem[5], and OMA(open mobile alliance) DRM[7]. The UltraViolet ecosystem is built by the consortium of major film studios and more 70 members. It supports the sharing of content between user devices as cloud-based digital authentication technology and also it allows the share of content between members by applying the concept of domain to family members. The UltraViolet ecosystem's main roles are composed of the Coordinator, DSP(download Service Provider), LASP(Locker Access Streaming Provider), Retailer. In particular, the Coordinator controls and manages DRM Domain, Device, Rights, etc. For more details, refer to the [12].

The Marlin DRM is made by MDC(Marlin Developer Community) of five companies that are intertrust, Panasonic, PHILIPS, Samsung, and Sony. It targets the only truly interoperable and open digital content sharing platform. The Marlin DRM system consists Web Store, Back Office, Marlin Server, and Marlin Client. By using Action Token and Business Token that include some commands and business logic, it controls the usage of content and management the license of content. Also the domain is managed by using the concept of Node and Link. For more details, refer to the [4].

The PlayReady ecosystem of Microsoft consists of PlayReady Severs and PlayReady Client. The PlayReady Servers are classified into the Distribution Server, Metering Server, License Server, Domain Controller, and Packaging Server. When the user plays the DRM-protected content, the PlayReady Client downloads the content and header from the Distribution Server. The PlayReady Client have to install the proper DRM software called as IBX(individual black box) before the downloaded content is encrypted. If there is not the proper DRM, it must be downloaded from IS(individual server). After then, acquisition of license and domain registration is performed and the content can be played. Refer to the [6] for more details.

The OMA DRM for mobile devices is recently released to Version 2.2. It targets the mobile devices and provides the trusted and secure service where the content is offered to mobile devices for a variety of service scenarios. For more details, refer to the [8].

3 Model of DRM Cloud

The goal of DRM Cloud is to provide some resources and functions to be required for DRM such as content packaging, license management, and key management and domain management. The Figure 1 shows the conception of DRM Cloud that consists of the Smart Devices, the Media Cloud, the DRM developer, and the DRM Cloud. In particular, A core part of Figure 1 is the DRM Cloud that provides the cloud consumers with the services for DRM. The subsection 3.1 describes the cloud consumers of DRM Cloud and their roles, and then the architectural layers which compose the DRM Cloud are described in subsection 3.2.

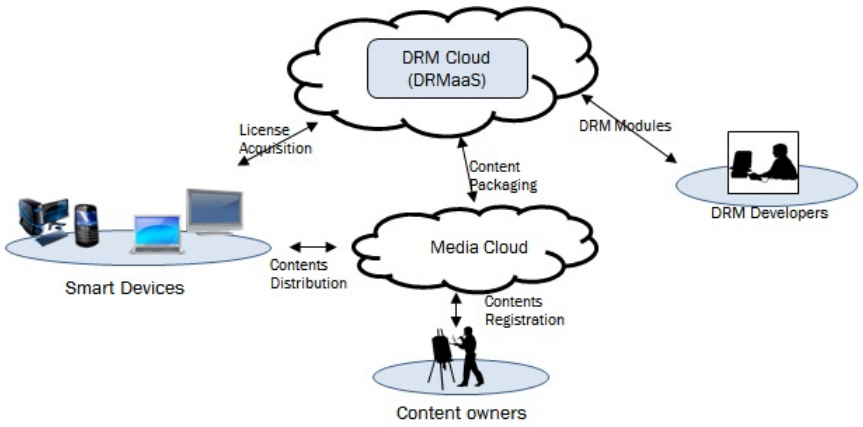

Figure 1: Conceptual Model of DRM Cloud

3.1 Cloud Consumers

As shown in the Figure 1, the cloud consumers for DRM Cloud are the Smart Devices, the Media Cloud, and the DRM Developers. Their roles are described as follows.

- Smart Devices: It is digital devices, which are owned by content users, that the purchased contents are played. In order to use the content, they have to make a request for the license at the DRM Cloud.
- Content Owner and Media Cloud: The Content Owner(CO) is the entity that owns the right of contents and registers some contents to the Media Cloud. The Media Cloud is the entity who takes responsibility for the content distribution. It provides the content downloading or streaming service and performs some procedures of content registration for some COs and content purchase for content users.
- DRM Developers: The entities that some components for DRM Cloud are developed using APIs provided by DRM Cloud or developed by themself. Then they offer the developed components as services of the DRM Cloud.

The cloud consumers of DRM Cloud demand for not only the services for DRM and but also the resources to be needed to provision the DRM services, and the DRM Cloud is composed of several components and layers so as to handle their demands. More details are described in the following subsection 3.2.

3.2 Architectural Layer of DRM Cloud

Some functions of DRM such as the content packaging, the license management, the key management, and the domain management are offered by the DRM Cloud, and in order to apply a variety of service scenarios to the DRM Cloud, management of the contents, various metadata for contents and the rights of usage policy are fulfilled by the Media Cloud. Thus the DRM Cloud is composed of the applications, several components and layers for controlling DRM functions. The Figure 2 presents the architecture of DRM Cloud which consists of four layers as follows.

Application Layer: This layer provides some applications for interface between the cloud consumers and the DRM Cloud. This layer can be regarded as SaaS(software-as-a-service) from the point of view of

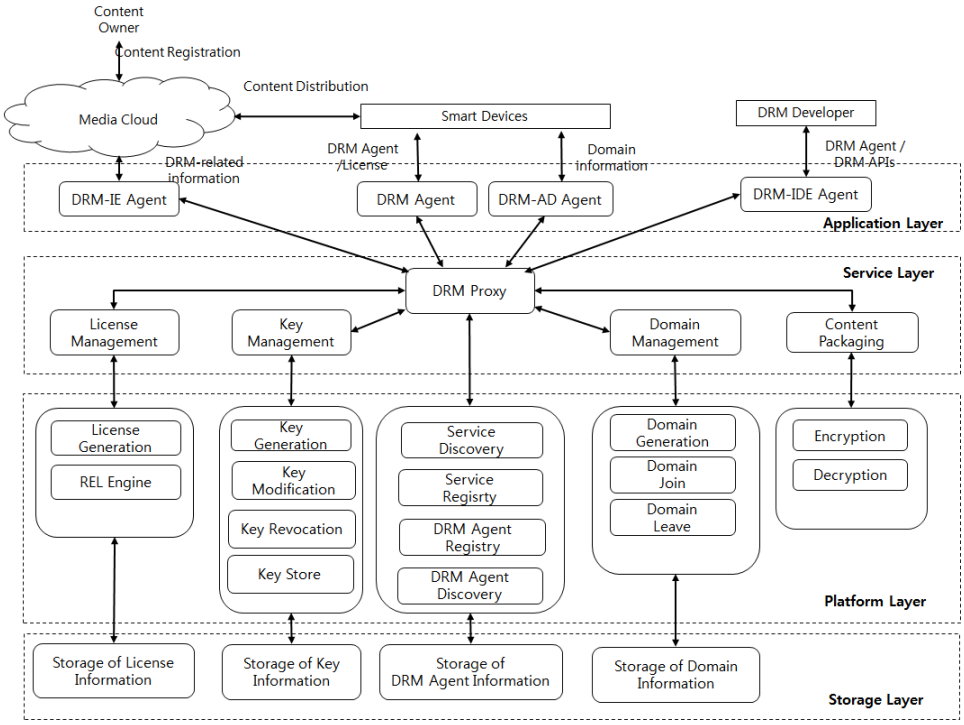

Figure 2: Architectural Layers of the DRM Cloud

the cloud service model. The cloud consumers can be provided with DRM services through the following applications.

- DRM-IE Agent for the Media Cloud: In the DRM Cloud, the content owners themselves select one of DRM technologies to be applied for content protection. For this, the DRM Cloud should provide a set of information about DRM for the content owner through Media Cloud. When the content owner registers the content, the Media Cloud utilizes the DRM-IE(integrated environment) Agent in order to offer some DRM-related information to the content owner and send a request the content packaging to DRM Proxy.

- DRM Agent for the Smart Devices: The content player for the Smart Device is based on SaaS. The DRM Agent is a DRM module that is included in the player and controls all of DRM services in order to use the content. The DRM Agent consists of license parser, decryptor, etc. This application is developed and offered by DRM developer.

- DRM-AD Agent for the Smart Devices: It is necessary for the Smart device to be joined in the domain for content sharing. The procedures related with the domain handling include the creation of domain, the join and leave of smart devices. Thus the DRM-AD(authorized domain) Agent is an application to provide the interface between the Smart Devices and the DRM Cloud for these procedures.

- DRM-IDE Agent for DRM Developer: The DRM developer develops the DRM Agent and some components of DRM services by using the DRM Cloud. For this, DRM Cloud provides DRM-IDE(integrated development environment) Agent as the IDE tools for DRM Developer.

Service Layer: This layer is in charge of the management of DRM service and the provision of practical DRM services.

- DRM Proxy: This component is a core part that manages DRM services. By using the DRM Proxy, the DRM services are managed, controlled and are provided for the consumers.
- DRM Services: This parts run a real instance for DRM services that are developed and published by the DRM Developers. And various practical DRM functions are invoked by the instance of DRM services.

Platform Layer: This layer provides APIs or components for some fundamental DRM functions which are the license generation/modification, the generation/modification/store of encryption key/license key/-domain key, the creation/join/leave of domain, and the encryption and decryption for content packaging etc.

Storage Layer: As shown in the Figure 2, this layer stores and manages some information about license, key, domain, DRM Agent and misc. These information are needed to perform DRM functions.

3.3 Service Scenario for Content Download Service

In this section, the content download service is described as an example of service scenario. In this scenario, the use of content is allowed on some devices registered in the domain. For sharing of contents in multiple devices, the domain is classified into two types, one is a *Family Domain*(FD) and the other is a *Personal Domain*(PD). The former means the group of devices that the family members are accessible to, and the latter is the group of devices in which the only specific member is accessible to some contents. Within the DRM Cloud, the Media Cloud takes charge of the management and distribution of contents. In other words, the Media Cloud's role does not include the management for DRM functionality. The goal is to allow the Media Cloud to concentrate on the content management and distribution to make the content service stable. The COs can select various content service providers as the the distributors of content from the Media Cloud because the content service providers can be a consumer of the Media cloud.

3.3.1 Content Packaging for Content Registration

For the content registration, the content owner connects to the Media Cloud that takes responsibility to manage and distribute the content of the CO. The Media Cloud must request for content packaging to DRM Cloud while registering the content. As shown in Figure 3, the content packaging is performed by requesting the services of DRM Proxy, the content packaging service(CPS), and the key management service(KMS), sequentially.

1. After connecting to the Media Cloud, the CO sends the content and its information to be registered to the Media Cloud.
2. The Media Cloud has to request for the content packaging to the DRM Cloud while performing the content registration. The Media Cloud sends automatically the information for content packaging by using the DRM-IE Agent which is received the from DRM Cloud as application.
3. After receiving the information for content registration through the DRM-IE Agent, the DRM Proxy invokes an instance of CPS to run the content encryption. Since the content encryption key(CEK) is required for content encryption, the DRM proxy has to request KMS for the key

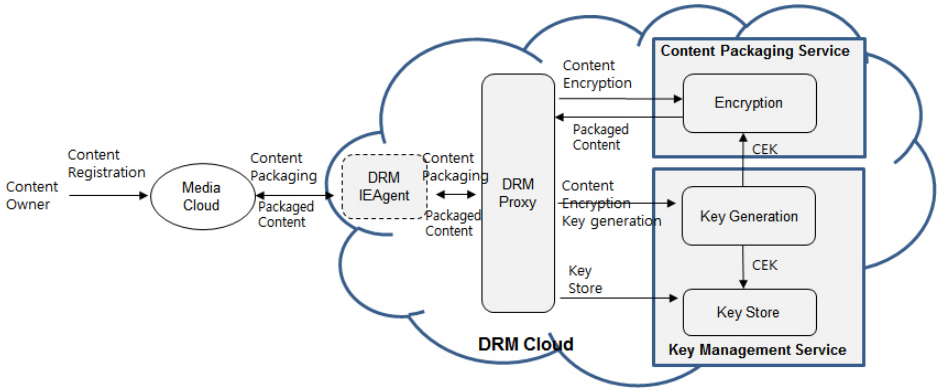

Figure 3: Content Packaging Service in the Process of Content Registration

generation. The KMS generates the CEK and stores it with the related key information for key management in the future.

4. After completing the content packaging, the DRM Cloud sends the packaged content to the Media Cloud via the DRM-IE Agent.

The content user connects to Media Cloud and purchases the content. The content is downloaded into one of Smart Devices which are owned by the content user. For the Smart Device to play the content after download, it have to request the license if it does not exist. In DRM Cloud, the license acquisition is performed as follows.

3.3.2 License Acquisition for Playing Content

The Figure 4 shows the procedures of the acquisition of license for playing the content. When the user selects the content to be played, the Smart Device receives the content player from the Media Cloud. In the content player, the DRM Agent must be included to request the DRM services of the DRM Cloud. In addition to this, if the Smart Device is not a member of domain, the device must be registered in the domain before requesting the license acquisition. The more details about the domain are described at the following subsection 3.3.3. After the content player is provided, the license acquisition is performed as follows.

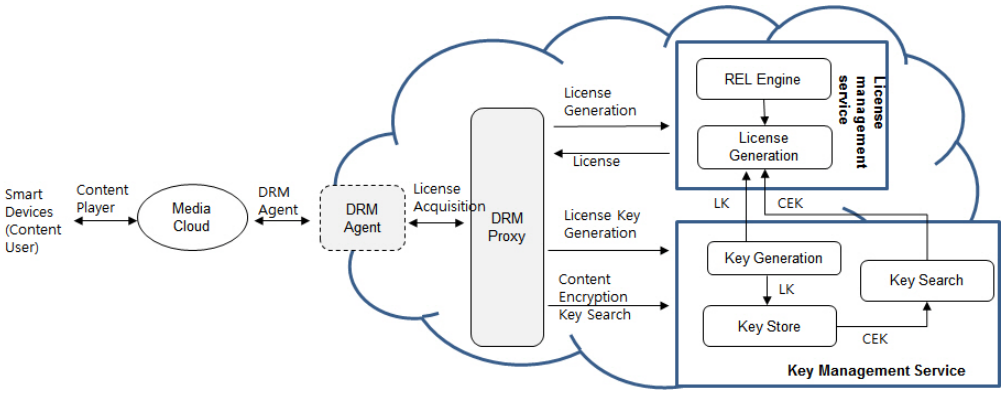

Figure 4: License Generation Service in process of License Acquisition

1. The DRM Agent checks the existence of license for playing the content. If there is no license for the content or it was expired, DRM Agent sends the request of license acquisition to the DRM Proxy. The DRM Proxy that received that request makes a request for the usage right(UR) to the Media Cloud since the DRM Cloud does not manage the UR.

2. After receiving the UR from the Media Cloud, the DRM Proxy invokes the instance of the license generation module through license management service(LMS). The LMS requests the two key, CEK and LK(license key) to KMS. The CEK used to encrypt the content in the procedure of content packaging is sent to LMS so as to include it into the license. For this, the KMS searches the CEK by using Key Search and then transfers it to the LMS through the DRM Proxy. The license key(LK) to be used to encrypt the the CEK is generated by the KMS. The CEK is encrypted by the LK so that only the user who have the license is allowed to play the content.

3. The license is generated by the instance of the license generation module and REL(rights expression language) Engine, by inputting the UR, CEK, and LK. After then, the generated license is downloaded to the Smart Device through the DRM Agent.

4. When playing the content, the downloaded license has to be verified by the DRM Agent. If the verification succeeded, the DRM Agent decrypts the packaged content and sends the decrypted content to decoder for rendering it.

3.3.3 Domain Management for Content Sharing

We describe more details about the concept of domain for the Personal and Family Domain. As described in the above, the *Family Domain*(FD) consists of a set of smart devices which all family members are accessible to. Thus all devices that are located in the home must belong to the FD. In the FD, there are several devices that are owned by each individual of family members, and a set of these devices is called as the *Personal Domain*(PD). As shown in Figure 5, for example, the FD is composed of all devices

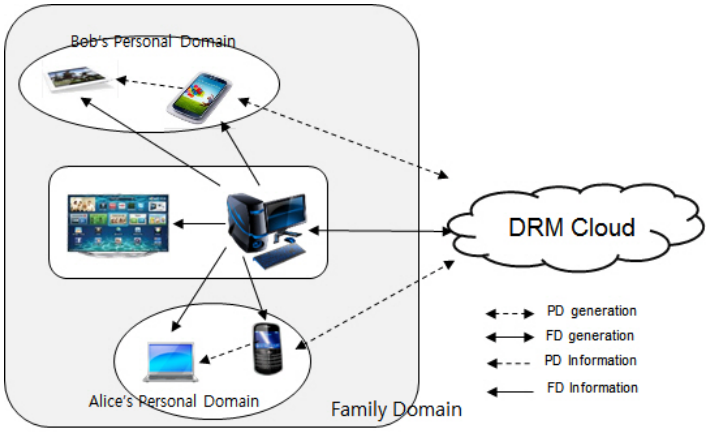

Figure 5: Concept of the Family and Personal Domain

in home and the two PDs is composed of the several devices that are individually owned by Alice and Bob. For example, the PC makes a request for the FD generation at the DRM Cloud and then stores the information of FD that are sent from the DRM Cloud. After then, another devices can join to the FD by getting the FD information from PC. If Bob(or Alice) wants to create only his PD, he has to request the PD generation at the DRM Cloud using one of his devices. After the PD is being generated, he transfers

the PD information to other devices for joining it to the his PD. More details for domain generation and join are described in the following paragraph.

Domain Generation: When the device connects to the DRM Cloud for a request of domain generation, the DRM-AD Agent is provided as the application through the DRM Proxy. There is no difference between the domain generations of the FD and the PD except the addition of a set of information for the PD. There requires the device information such as the ID of device and credential information what is needed to create and verify the two domains respectively. The processes of the FD generation consists of the generation of family domain ID, a FD master key, and the FD key. Particularly, the FD key is generated by the FD master key.

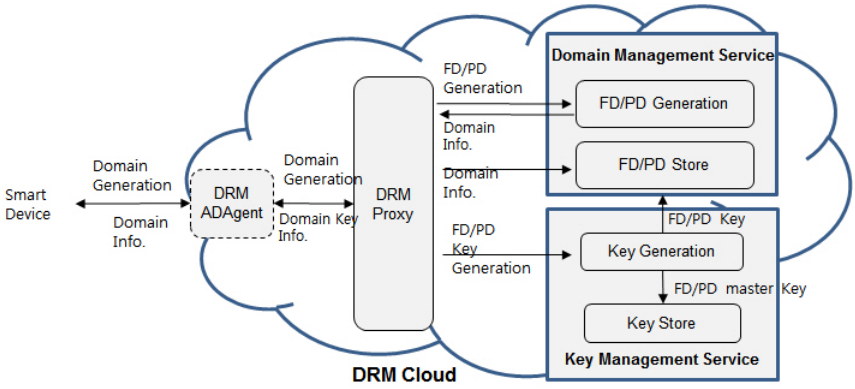

Figure 6: Domain Generation

1. The device sends the request of the FD generation to the DRM Proxy via the DRM-AD Agent along with the device information. The DRM Proxy invokes the domain generation function using domain management service(DMS). After creating the family domain ID, DMS calls the KMS for generating the FD master key and the FD key.
2. After the KMS receives the information to be needed for generating the key from DMS, it generates the FD master key and the FD key using pseudo random function within key generation module and then stores these key information.
3. The DMS receives the information related to the FD including the FD key from KMS through DRM Proxy and then store it. After then, it transfer the FD information to the Smart Device.
4. The process of domain generation is ended after storing the domain information to the Smart Device.

The domain generation of PD is similar to that of FD except that the family domain ID is needed when requesting the generation. Also the PD master key and personal credential information are used instead of.

Domain Join: The process of domain join is to register a smart device to the FD or the PD. This means that the device ID is stored into the database of DRM Cloud which is managed by DMS. Figure 7 shows the process that the Smart Phone requests for the Domain Join to the FD. Assume that the PC has the domain information because the FD is created by the PC. Before sending the request to the DRM Cloud for join, the Smart Phone has to connect to the PC to get the family domain ID.

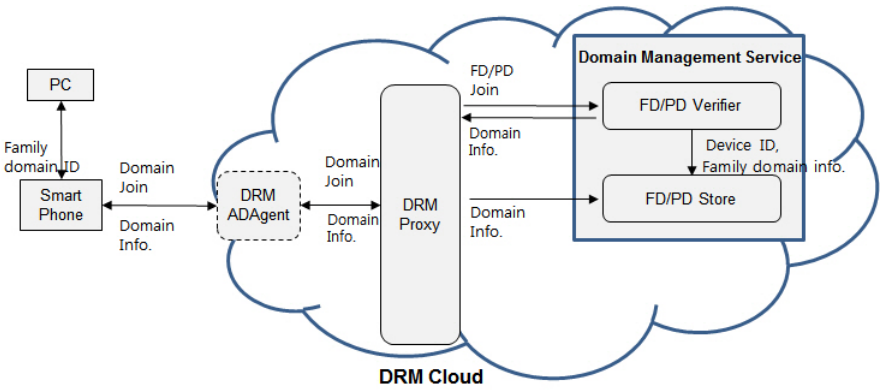

Figure 7: Domain Join

1. The Smart Phone connects to the PC and requests the family domain ID.

2. The Smart Phone transfers the device ID, the credential information and the family domain ID to the DRM Proxy via the DRM-AD Agent. After receiving the join information, the DRM Proxy sends these information to the DMS with the request of domain join.

3. The DMS verifies the credential information. If verification succeeded, the DMS stores the family domain information and the device ID as a pair to the database of storage layer at the DRM Cloud. Since the family domain information and the device ID are associated with each other, it is able to know the family domain where the device belongs to.

4. The DMS sends the FD information to the Smart Phone. The process of domain join is ended after the Smart Phone stores the received information.

The domain join to the PD, like the domain generation, are similar to that of FD except that the personal domain ID, the PD information, and personal credential information are used instead of.

4 Discussion

In this section, we discuss the establishment of trusted DRM Cloud and compare the proposed model of the DRM Cloud with the existing methods. Also the advantages of the DRM Cloud are described. In order to offer the trusted DRM Cloud, the following things should be assured.

- All entities have the unique public and private key pair and the certificate issued at the time of device manufacturing, installing of some components, or service subscription.

- The communication between the entities within same cloud infrastructure should be protected by secure channel.

- The trust between the cloud consumers and the DRM Cloud should be established. That is, the communication of these entities is secured by sharing the information for the establishment of secure channel in the process of the service agreement.

- The Content Owner and the Media Cloud are protected by hybrid cryptographic method that combines the public and symmetric encryption.

- The communication between the Smart Devices and the Media Cloud as well as between the Smart Devices and the DRM Cloud should be protected using hybrid cryptographic method.

When the services to be provided by the cloud are changed, the rapid upgrade of service is necessary and the effect of changes on the system must be minimal. For the purpose of this, the cloud aims the modular architecture that decomposes certain function to the several modules as possible. In other words, the higher the modularity of function is, the more flexibility the Cloud can provide. From this point of view, we compare the proposed DRM Cloud with UltraViolet, Malin DRM, and PlayReady which are described in the Section 2. The Figure 8 shows the mapping diagram between the DRM functions and the entities which take responsibility for these functions. This mapping diagram means that the several modular of DRM function are intensive on certain entity or the another entities are needed to run one of DRM functions, so it decreases the independence of system. As a result, the elasticity and flexibility of system become to decrease. In the DRM Cloud, there is a one-to-one correspondence between each DRM function and each entity. Thus they are irrelevant to each other even if modified. Therefore, the DRM Cloud can be more elastic and flexible than the existing methods.

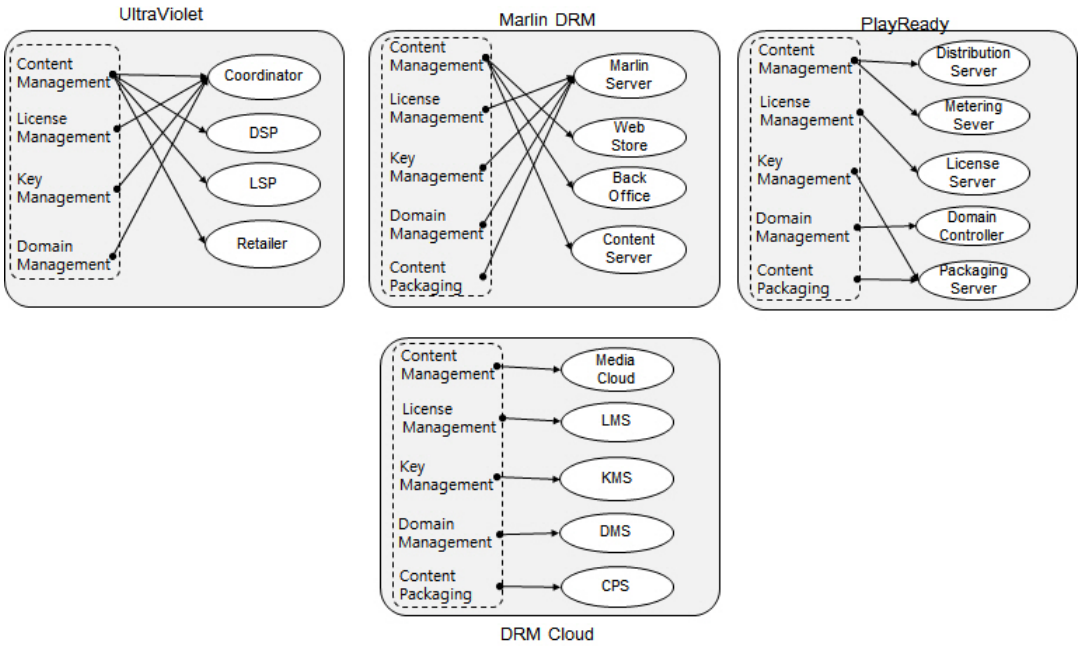

Figure 8: The Mapping diagram of DRM functions and the entity in the DRM Technologies

From this discussion, the advantages of DRM Cloud are described as follows.

- The Media Cloud needs not be cost for building DRM system, and can support the several DRM technologies or can be changed any time.
- The Smart Device is given the DRM Agent as SaaS which is suitable to his device or DRM-protected content, so the Smart Device does not depend on specific DRM technology. As a result, the purchased contents can be persistently used even if the content user has changed the Smart Device built on different platform.
- The DRM developers can just utilize the fundamental functions of DRM Cloud as it is. Thus they can reduce the time and the costs for development.

5 Conclusions

In this paper, the concept of DRM-as-a-Service based on the cloud, the architectural layers, and the service procedures for the content download service are proposed. Also we discuss some concerns for establishment of trusted DRM Cloud, comparison with existing DRM technologies in aspect of flexibility, and several advantages of the DRM Cloud. The DRM Cloud allows the content consumers to play some DRM-protected contents in various smart devices, and for the content service providers it allows to apply various service scenarios. And the DRM Developer is allowed to develop the DRM solutions with low cost. As a conclusion, the DRM Cloud has several advantages for cloud consumers. But, in this paper we dealed with concepts of DRM Cloud architecture and service scenario only. As further study, it will require some researches about technical requirements, system capability required , security, performance, details of implementation for DRM Cloud, and so forth.

References

[1] D. D.-S. et. al. Media cloud: An open cloud computing middleware for content management. *IEEE Transaction On Consumer Electronics*, 57(5):970–978, 2011.

[2] D. Mains and T. Neumayr. Apple unveils higher quality DRM-free music on the iTunes store. `http://www.apple.com/pr/library/2007/04/02Apple-Unveils-Higher-Quality-DRM-Free-Music-on-the-iTunes-Store.html`, April 2007.

[3] Marlin. `http://www.marlin-community.com`.

[4] Marlin broadband architecture overview. white papers. `http://www.marlin-community.com/develop/downloads/white_papers`, 2006-2011.

[5] Microsoft playready - home. `http://www.microsoft.com/playready`.

[6] Microsoft playready content access technology. white paper. `http://www.microsoft.com/playready/documents`, July 2008.

[7] Open Mobile Alliance. `http://www.openmobilealliance.com`.

[8] OMA Digital Righst Management V2.0. `http://technical.openmobilealliance.org/Technical/release_program/drm_v2_0.aspx`, 2012.

[9] Z. L. P. Zou, C. Whan and D. Bao. Phosphor: A cloud based DRM scheme with sim card. In *Proc. of the 12th International Asia-Pacific Web Conference (APWeb'10), Busan, Korea*, pages 459–463. IEEE, April 2010.

[10] M. Tan and X. Su. Media cloud: When media revolution meets rise of cloud computing. In *Proc. of the 6th IEEE International Symposium Service Oriented System Engineering (SOSE'11), Irvine, California, USA*, pages 251–261. IEEE, December 2011.

[11] UltraViolet. `http://www.uvvu.com`.

[12] DSystem:System Specification Version 1.0.6. `http://www.uvvuwiki.com/images/9/99/System-C1.0.6.pdf`, February 2013.

[13] Verimatrix Multirights. `http://www.verimatrix.com/solutions/multirights.php`.

[14] J. W. W. Zhu, C. Luo and S. Li. Multimedia cloud computing. *IEEE SIGNAL PRCESSING MAGAZINE*, 28(3):59–69, May 2011.

[15] Widevine DRM multiplaform content protection for internet video delivery. `http://www.widevine.com/wm_drm.html`.

Author Biography

Hyejoo Lee received her M.S. and Ph.D. degrees from Pukyong National University, Busan, Korea in 1997 and 2000, respectively. She worked as a senior researcher in Electronics and Telecommunications Research Institute, Daejeon, Korea from 2001 to 2005. She is currently working as Post Doctor in Department of Applied Mathematics at Kongju National University, Gongju, Korea. Her research interests include digital righst management, digital watermarking, multimedia protection,and image processing.

Changho Seo received his BS, MS, and Ph.D. in 1990, 1992, and 1996, respectively, from the Department of Mathematics at Korea University, Seoul, Korea. Currently, he is a full professor in Department of Applied Mathematics at Kongju National University, Gongju, Korea. His research interests include cryptography, information security, and system security.

Sang Uk Shin received his M.S. and Ph.D. degrees from Pukyong National University, Busan Korea in 1997 and 2000, respectively. He worked as a senior researcher in Electronics and Telecommunications Research Institute, Daejeon, Korea from 2000 to 2003. He is currently an associate professor in Department of IT Convergence and Application Engineering, Pukyong National University. His research interests include digital forensics, e-Discovery, cryptographic protocol, mobile/wireless network security and multimedia content security.