A Novel Approach towards EDRM System Design for Android Device

Harshala Yadav
Thakur College of Engineering and Technology
Mumbai, India

ABSTRACT
As digital content services gain importance in the mobile world, this paper proposes Digital Rights Management implementation for android devices. EDRM (Enterprise Digital Rights Management) system provides a novel solution to control access to documents such as Microsoft word, PDF and images from unauthorized copying, modification, and re-distribution. The work protects user's personal digital content like photos, documents etc. This modeled design aims how security is been provided to mobile devices using password mechanism, hash function and encryption and it is been tested using 100 samples. The individualization, flexibility, efficiency and practicability issues will be assured. The implementation permits the mobile user to conduct a 'preview-before-download' activity and the digital content provider will not suffer from unauthorized mobile users accessing digital content. Proposed system uses a two level security using a Universal Unique Identifier, which is hashed using the (Simple Hashing Algorithm) SHA algorithm, then that key is used for the encryption of the content in Advanced Encryption Standard (AES) algorithm. The parameters used to measure system performance are response-time and throughput and were found out to be 0.022-sec/request and 45.54 respectively. Thus the paper achieves better security and faster processing.

General Terms
EDRM, Android, DRM, Digital, Security, Encryption

1. INTRODUCTION
Digital data has become an integral part of the modern world. Generation and usage of digital documents like PDF, docs and images has an incremental growth and has a central role in everyday life, be it business, education or personal. Our dependency on digital information has increased so much that digital documents have to be accessed from anywhere and anytime on personal devices such as smartphones, tablets and public desktop machines. Technologies such as 3G, 4G, Wi-Fi, smartphones and tablets have made it easy to access and utilize data. However, security and more importantly privacy of data is of primary concern.

Information should be available anywhere and anytime (even for offline use) but data should remain secure and privacy should be retained. Besides the technical aspects of storage and sharing, data complexity has increased and so has the complexity of data security and privacy. Data is stored, accessed and shared now on various mediums like USB flash drives, public servers, personal desktops and laptops, smartphones and more recently on cloud. On all these mediums data security is regularized by usage of hashing algorithms such as SHA-1, SHA-2 and encryption algorithms such as DES, AES etcetera. Data privacy is regulated with respect to sharing of data with authorized users, copyright protection. A termed coined for securing such data files and maintaining their privacy in regards to sharing with authorized users is 'Digital Rights Management'.

Some of the important concepts of Digital Rights Management are usage control (content provider may wish to control how the user is handling the content), access control (allowing only a certain group of authorized users to access data) and data consistency management. In the current world smartphones and such similar devices have begun to replace traditional systems to store, access and share data. So, in this article we would be targeting hand held devices such as smartphones and follow an object oriented approach to encapsulate within a document a security mechanism to secure it and to have a control on its usage and sharing as well preserve its privacy.

The remainder of this paper is organized as follows: Section 2 presents a prerequisite in terms of a literature review; Section 3 describes a planned approach to the EDRM system for android devices; Section 4 provides an implementation solution and encryption and hashing; Section 5 shows outcome of the system; the conclusions and future directions are presented in Section 6.

2. LITERATURE REVIEW
Chen-Yuan Chuang; Yu-Chun Wang; Yi-Bing Lin; (2010) [1] Android is an open mobile phone platform. Author has suggested accommodating value-added services such as selling wallpapers, ringtones, applications, and games on Android phones; it is extremely important to ensure copyright protection on these products. Here OMA DRM is used to implement Android source code. Author also identifies potential leaks of Android DRM and software protection.

Liang Wang; Chen Wang (2013) [2] According to the concepts defined in paper, author got a DRM solution based on OMA DRM 2.0 and mobile devices' characteristics. Application of this technique is suggested is mobile digital journal. Author has also paid attention on the security mechanism. For security author has used asymmetric key cryptography. Intellectual property rights is major concern, protect that copyright has came into picture.

The Open Mobile Alliance (OMA) [3], which is device-based and works to define industry-wide specifications for applications that operate over wireless communication networks, has already released a version two DRM specification. The scope of their specifications enables the controlled consumption of digital media objects by allowing content providers to express usage rights (e.g., the ability to preview the valuable content) to prevent downloaded DRM content from being illegally forwarded (copied) to other users and enable super distribution of DRM content.

Existing DRM system [4]:

Apple

Apple computers introduced ITunes as a music store and later on expanded the product category to movies and now to E-books. ITunes is an application level DRM controller and it is an interface among the apple products. ITunes allows a user to register up to five Apple devices.

Rights Management Services (RMS, Microsoft [5][6])

Rights Management Service is developed by Microsoft and is mainly developed for enterprise purposes. This DRM system is the only system that has access control support in operating systems kernel. RMS protects all types of data and is mostly used in enterprises. RMS is device-based system.

Adobe DRM (Adobe)

Adobe was the first to implement a DRM in the consumer space. Adobe's DRM is mostly used for Adobe's formats therefore this DRM system can only support PDF. On the flip side this DRM system is capable of supporting a wide range of platforms on embedded as well as desktop systems. But Adobe's DRM is not capable of controlling the distribution of illegal copies.

Kindle

Amazon launched its first eReaders in 2006 and since then is increasing sales of eBooks from kindle store by introducing new eReaders and tablets. The eBooks sold from the kindle store are protected by kindle's DRM. DRM policies of Kindle are not appreciated a lot by kindle users because of the user privacy issues and format support issues.

3. PROPOSED SYSTEM

The system put forward an EDRM mechanism, which will prevent unauthorized use of the digital content. System design is based on two important ideas. The first idea focuses on the client-side, where EDRM system does authentication of client via password and IMEI number of the android device. The second idea focuses on the server-side, where author authentication is checked and the identity of user of the android device. Only when an Android device user clears the verification the digital content can be retrieved. System makes use of symmetrical cryptosystem in the solution. Cryptosystem is used for the security of the digital content.

When an Android device user enters a correct password, the user can access EDRM system. User should be able to check all the files, which is of his interest. Before downloading any content system should allow a user to see the preview of the file, so looking at the preview user should decide if he wants to download the content for his use [7][8]. So download request should be put to server side if he clears the entire authentication user can freely access the content. Different plugin should be supported by the system so that content can be seen.

(1) The Author or user creates valuable personal digital content and then sends it to the File management module.

(2) The File management encodes the digital content to a DCF (it includes the encrypted content) and generates a symmetric encryption key to encrypt the digital content. Afterward, the DCF is stored in a public directory of the Content Server (CS) for related mobile users to download it.

(3) The File management sends the decryption key to the Rights Management (RM) to manage the digital rights.

(4) The mobile users use a Mobile Terminal (MT, for example: mobile phone or personal digital assistant) to establish a connection channel with the CS and download the DCF.

(5) The mobile user previews the digital content. If it is interesting to the mobile user, he then proposes a download request to the Rights management module. Upon receiving the mobile user's request, the User Management Module (UMM) verifies the mobile user's identity. The UMM also verifies whether the mobile terminal is legal or not.

(6) UMM maintain descriptive meta-data such as author, title and a URL the user may visit in order.

(7) The UMM forwards the protected decryption key to the mobile user.

(8) After receiving the digital content, the mobile user tries to open the downloaded digital content, the EDRM System uses the decryption key to decrypt the digital content and requests the mobile user to enter the password before starting with the mobile EDRM system and checks for the IMEI number of the mobile device. Only when the user has cleared both authentications; user gets the decryption key. Therefore, EDRM system can access the digital content; otherwise the access will be denied.

4. IMPLEMENTATION

The proposed EDRM solution is providing Digital rights management implementation for android devices. The novel design model protects user's personal files like photos, images, .doc file and .PDF documents. The planned system gives a mobile DRM solution that protects the digital content. Solution is based on two important ideas. The first focuses on the client-side, which is authenticated via password. The second focuses on the server-side, which is dependent upon the mobile terminal and the mobile user identity authentication. Only when the mobile terminal and the mobile user pass authentication, can the digital content be accessed. The system also utilizes a SHA- 1 and symmetrical cryptosystem in implementation.

Once the mobile user enters the correct password, the embedded EDRM system can only retrieve the decryption key. A "preview" model should be involved in the mobile DRM system. That is, anyone can preview digital content in advance. If the digital content is interesting to the mobile user, the mobile user downloads the related EDRM system and proposes a request to the rights issuer. Simultaneously, a well-designed DRM should integrate existing mobile unit applications such that the various EDRM system types (such as players, viewers or readers) can manage the various applications.

Figure 1 explains about the architecture of the EDRM solution, which is been implemented to achieve security for the personal documents. It describes module wise working of server as well as client side. There are four modules that are implemented on server and client side. Database of EDRM is stored Sequel Pro, where three data sets are been created.

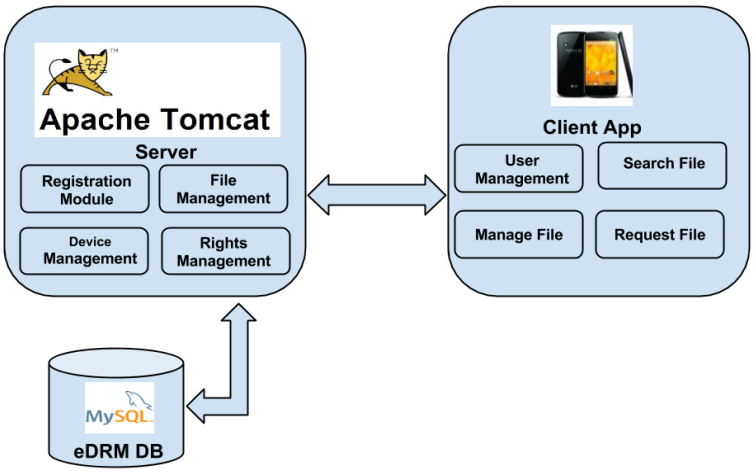


Figure 1: Architecture of EDRM system

4.1 Modules

4.1.1 Server side

Registration Module:
An author who wants to store their data on the network they can register through web. In the system expected fields to be complete while registrations are name, address, email-id, phone no, city, state and zip. Once the user complete with registration process, he can use his mail- id and password to login through web. Now he has full access to upload his content onto the server using File management module. He can upload image, doc file, and PDF document.

Device Management Module:
When client side user wants to access system first he downloads the system on his android device. Client has to register through device and verification is done at the server side. All the required fields are filled properly then user gets the authentication to use email ID and password to login through android device.

File Management Module:
When author logins through web, he can upload word document, images and PDF files. For uploading an image file he has to browse from the system and select the file, which has to be uploaded. Once the image file is uploaded in two formats one is original file and other is scaled image, which is shown while previewing the image file. Image file can be of type's .jpg, .jpeg, and .PNG.

For uploading word file or PDF document along with the title user has to enter preview text about the content looking at which user will decide whether the content is relevant to his search. After viewing the preview content user downloads the file which is in the encrypted format and seen only through our EDRM system.

Rights Management Module:
Authenticate a user to share the file with the device it has requested from. When users preview the file and if he is interested in the content he downloads the file. Device management checks the IMEI number of the requested user and if it is register then user gets the content on his device. But the content will be kept in the encrypted format and it will be open through our EDRM system. User can read the content but he can't copy paste, forward the content. Even if someone tries to get the content he will not able to decode the content because it will be in the encrypted format.

4.1.2 Client side

User Management Module:
User downloads a system into the device and register through the system. While registering the IMEI of the device is stored into the database. When user uses login id and password on the device, server side Device Management Module will check for authentication credentials that are stored in the database and if it matches then it authenticate user to use the system. There will be one account for single user if he tries to login through different device on the system while authenticating credential fails pop up will come because stored IMEI will not match to the device IMEI number.

Search File Module:
When user clears with the authentication procedure, he can search the file according to his requirement so there are options that he can select are search by type, search by name and all files. According to the search of user the content will be shown to the user. Metadata of the search query is sent to the content server.

Manage Files Module:
Once user login to the system he has full authentication to use system and if he wants to view downloaded files he can just check for the files it will show all the files which are downloaded. All this downloaded files can be viewed from our EDRM systems only using appropriate readers for .doc and .pdf files.

Request File Module:
Once user login to the system he has full authentication to use the system and if he wants to view requested file but not downloaded because he did not find it relevant can be seen. Preview of the file will be provided by the system. And further if he wants to download then directly he can download from there itself.

4.2 Encryption And Hashing

As we are facing problems on security we need to secure our document with help of new encryption algorithms and hashing techniques. As study has proved Advanced Encryption Standard (AES) secures the content as compare to other encryption techniques. AES is an encryption algorithm used to encrypt electronic data. It is symmetric key algorithm works on different key and block size. It works on block size of 128 bits but with the different key lengths: 128, 192 and 256 bits. Implementation of EDRM system uses 256-bit key length to provide maximum security. Using this we can secure TOP SECRET data of the user will be secured with the help of 256-bit key. AES has 14 cycles for 256 bit keys.

Hashing technique used in the implementation is a SHA-1, which is a Cryptographic hash function produces hash value. Globally unique identifier (GUID) or Universally unique identifier (UUID) is used as an identifier which stores value as 128 bit values. This unique identifier is used for the files, which are supposed to be stored on the database. With the help of UUID we have different identifier for all the uploaded files. SHA-1 hash function is applied on UUID to generate the key that is used for the encryption of the uploaded file. Encryption is used for securing the uploaded content, which may be a TOP SECRET data.

International Mobile Station Equipment Identity (IMEI) is unique identifier of the mobile device, which is used to identify the owner of the mobile device. When user register in the EDRM system, along with the registration details IMEI of the user device is helpful in the security.

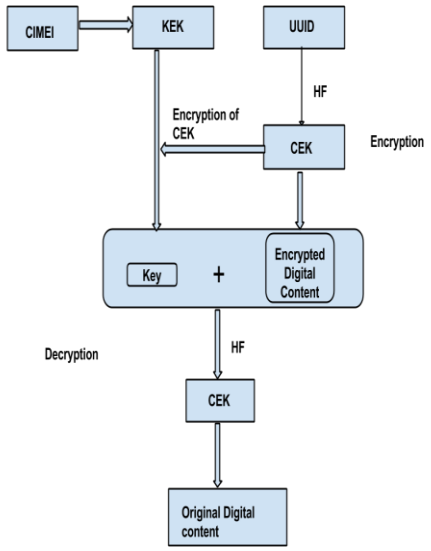


Figure 2: Working model using encryption and hashing in EDRM

(1) Author who wants to upload his files like images, documents he will use the File Management Module to upload a file from web. Each file will have unique identification number and it is stored in the database. This id is passed in the metadata when user wants to access this file.

(2) The file is uploaded to the server by generating a random UUID value. This value is unique to each file when uploading and that is the key of the file. The UUID is passed to the hashing function (SHA-1) to make key of 256 bits and stored as CEK. Using this nonce value we can encode the file and keep it in a database. Encoding is done using AES 256 bit algorithm to provide security.

(3) This UUID key is then stored in the database corresponding to the file for later use while decrypting on the client side.

(4) Client (user) requests the file form server using Search file module by sending his IMEI number.

(5) Client request for metadata services.

(6) The Server will then encrypt the UUID key, which is stored in the database using which the file is encoded, using the IMEI number of the device it has requested from. The IMEI number is sent to the hashing function to get 256 bits key and stored as KEK to encrypt the CEK using AES 256 bit algorithm.

(7) Client receives the file and User Management module will check for credential like IMEI number then decrypts the UUID at its end.

(8) And the file download is completed and an entry in user's local database is made to ensure file download was completed.

5. RESULTS AND DISCUSSION

Enterprise digital rights management (EDRM) shares the DRM's basic concept of controlling content use. The solution provided goes beyond unauthorized-copy protection to help sensitive information from being read, altered or shared outside one's scope while not interfering with the user's work.

The EDRM implementation provided above has the basic characteristic of security. IMEI is used as an input for key encryption. Thus, data and key are encrypted and the document has authorization before being used for previewing or offline viewing. The system is not harder to use than working with unprotected document. Lastly it is easy to deploy and manage since it is based on the android platform.

When users search a file by type, namely .jpg, .jpeg, .pdf, .doc all the files will be listed under those types. The jpg file is searched shown in figure 3.

Figure 3: Search by type

When users click on the file, preview of the image file will be available to user. In case of PDF and .doc file the preview text will be shown. If user is interested in downloading the content user will click on the download button, after that image gets stored into user's memory card. Figure 4 show that user can access all the downloaded files through EDRM System.

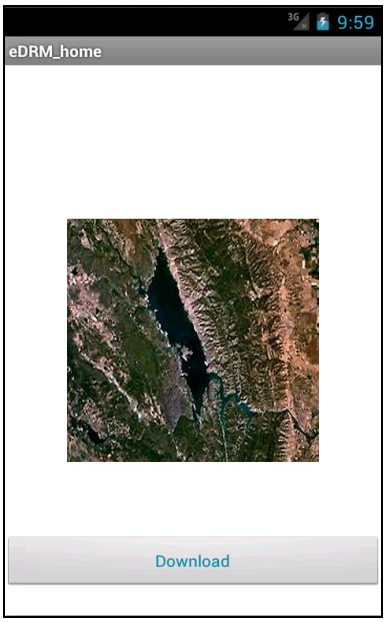


Figure 4: Preview of image file

User can view the entire downloaded file under downloaded tab to access as and when required by user is shown in figure 5. All the downloaded files have to be accessed trough EDRM system.

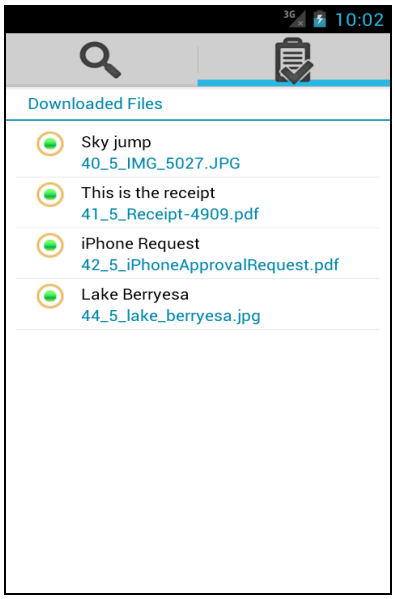


Figure 5: Downloaded files of users

When user tries to access the file from SD card where actually file will be located, without using the EDRM System, he will get an error message, because the file is in the encrypted format before viewing the file it has to be decrypted to use it shown in figure 6. So file can be accessed by pdfviewer which are used for PDF and .doc file. Images can be seen without any viewer. Even if file is send to any body it cannot be accessed because every time decryption key has to be taken from the server where other user will fail the authentication of the IMEI number.

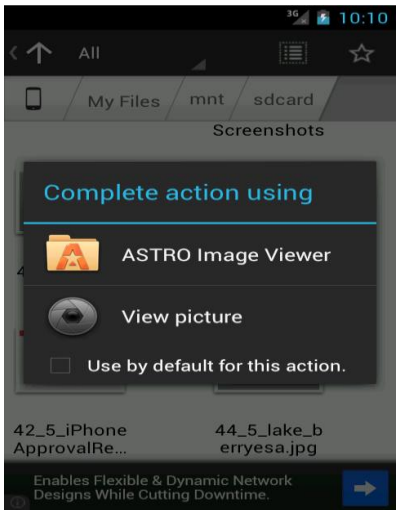


Figure 6: File access without EDRM System

When we examine the existing DRM system with EDRM system, comparison is shown in Table 1. It is clearly observed that EDRM system provides confidentiality with the help of different techniques, which are used in the development of the EDRM system.

Table 1: Comparison of existing DRM with EDRM System

EDRM Systems	Microsoft DRM	OMA DRM	EDRM System
System Architecture	Device Based	Device Based	Device Based
Participants	Content user, License Server, User	Content user, License Server, User	Author, Content Server, User
Right Access	Yes	Yes	Yes
Content Encryption	Yes	Yes	Yes
Confidentiality	No	No	Yes

Figure 7 shows the statistics of the server side pages, where 100 samples were taken and throughput achieved as 54.30, error rate is 0.06% and data rate achieved as 297.57 KB/sec.

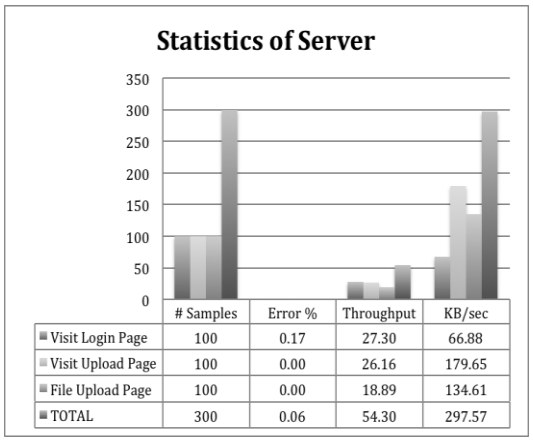
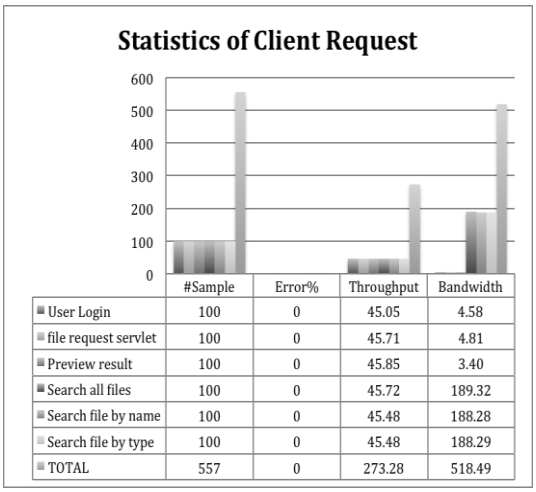


Figure 7: Statistics of Server

Figure 8 shows the statistics of six clients side web pages where 100 samples were taken, where throughput achieved as 45.54, error rate is 0% and bandwidth is 518.49.



	#Sample	Error%	Throughput	Bandwidth
User Login	100	0	45.05	4.58
file request servlet	100	0	45.71	4.81
Preview result	100	0	45.85	3.40
Search all files	100	0	45.72	189.32
Search file by name	100	0	45.48	188.28
Search file by type	100	0	45.48	188.29
TOTAL	557	0	273.28	518.49

Figure 8: Statistics of Client Request

6. CONCLUSION AND FUTURE SCOPE

This paper presented a novel model for protection of digital documents on mobile terminals. The implemented method has the following properties:

(1) Identification of user is done using the network special entity as IMEI for protecting illegal access to the digital document.

(2) The proposed model used a simple operations like hash function, password mechanism and cryptography.

As discussed at the beginning of this paper everyone is facing many problems: they want to secure their documents from getting fabricated and used somewhere, but even though documents must also be distributed among users. Enterprise Digital Rights Management architecture is the solution been provided in this paper. When user opens a document, the security is been provided on the android devices. Application of this EDRM architecture will be cloud storage for enterprise documents. The implementation gives throughput and response time of 45.54 and 0.022 sec/request; fairly acceptable for today's standards.

With Enterprise DRM for android, applying security policies that control that can view what documents. Additionally, Enterprise Digital Rights Management can restrict the copying and printing of documents. Thus EDRM persistent document protection is effective regardless of a document's physical location, and rights to content can be revoked after a document has been sent.

The system being tested with the sampled inputs, the proposed model can be scaled up to a real time implementation of EDRM system for android devices using a distributed approach. The system can be taken further with the challenges in distributed approach and implementation in the following areas:

(1) Enterprise content security is a top priority for all Companies, including the government. Looking at the current growth, smartphones in the near future will certainly play a fundamental role at every level in the human society. The current proposed EDRM model would have to be modified taking into account the large scale of the organization, larger number of inputs and complex security levels.

(2) Implementing EDRM on the commercial level would prove to be an effective way to protect confidential information and to prevent document leaks. The modified EDRM implementation will have to be done on a real time basis so as not to affect the availability and security of current implementations.

(3) The challenges for EDRM to work on such a large scale include recognizing the current securities implementations and policies of the organization at stake. The other important issues to be addressed are multi-level and multi-lateral security, connectivity, availability and urgency.

7. ACKNOWLEDGMENT

I would like to show my gratitude towards my project guide Dr. R R Sedamkar for his guidance and concern throughout the execution of this project.

8. REFERENCES

[1] Chen-Yuan Chuang; Yu-Chun Wang; Yi-Bing Lin; , "Digital Right Management and Software Protection on Android Phones," Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st , vol., no., pp.1-5, 16-19 May 2010 doi: 10.1109/VETECS.2010.5493648

[2] Liang Wang; Chen Wang; , "A DRM system for mobile digital journals based on OMA DRM model," Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on, vol.5, no.,pp.2310-2313, 12-14 Aug. 2011 doi: 10.1109/EMEIT.2011.6023573

[3] Open Mobile Alliance (OMA1), http://www.openmobilealliance.org/

[4] Vyas, Rohit. (2012) 'A rental Digital Rights Management framework which allows user to lend books and notes). MSc Thesis. University of Bedfordshire

[5] Microsoft Inc.1, Windows Media Digital Rights Management, http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx

[6] Microsoft Inc.2, Microsoft Window Right Management Services System http://www.microsoft.com/windows/windowsmedia/forpros/drm/default.mspx

[7] Chin-Ling Chen; An "All-IN-ONE" Mobile DRM System Design, International Journal of Innovative Computing, Information and Control, vol 6, no. 3(A), pp 897-911, March 2010

[8] Chin-Ling Chen; An "All-IN-ONE" Mobile DRM System Design,

http://ir.lib.cyut.edu.tw:8080/bitstream/310901800/7037/1/13.pdf

[9] Sye Loong Keoh; , "Marlin: toward seamless content sharing and rights management," *Communications Magazine, IEEE* , vol.49, no.11, pp.174-180, November2011 doi:10.1109/MCOM.2011.6069726

[10] Subramanya, S.R.; Yi, B.K.; "Digital rights management," Potentials, IEEE, vol.25, no.2, pp.31-34, March-April 2006 doi: 10.1109/MP.2006.1649008

[11] Chang, F.C., Wu, C.L. & Hang, H.M. (2007) "A switchable DRM structure for embedded device", Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on, IEEE p37-40.

[12] Cohen, J.E. (2003) 'DRM and privacy', Communications of the ACM, 46 (4), pp.46-49.

[13] Information Rights Management from Wikipedia

[14] C. Conrado, F. Kamperman, G. J. Schrijen and W. Jonker, Privacy in an Identity-based DRM System, Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03*)*, September.1-5, 2003,pp.389-395, 2003.

[15] W. B. Lee, W. J. Wu and C. Y. Chang, A portable DRM scheme using smart cards, Journal of Organization Computing and Electronic Commerce, Vol. 17, No. 3,247-258, 2007

[16] J. A. Onieva, J. Lopez, R. Roman, J. Zhou and S. Gritzalis, Integration of Non-repudiation Services in Mobile DRM Scenarios, Telecommunication System,Vol. 35, pp.161-176, 2007.

[17] Open Mobile Alliance (OMA2), mobile device DRM standard version two, http://www.openmobilealliance.org/release_program/index.html