Is Digital Rights Management a Means to An End?

Puspanjali Jena **Dipak Kumar Khuntia**

Abstract

Computer networks are a crucial part of organizations. It is one of the fastest growing technological areas and brings benefits virtually to every country in the world. With the interconnection of network to the Internet, the world has truly become a global village where we depend more, on digital materials. So in the present century all digital works need protection because they can be easily copied. For that reason DRM technology has taken place, which is not a single technology or not a single philosophy. It refers to a broad range of technologies and standards. DRM is neither thin nor thick copy right. DRM is potentially a planned technique for absolute protection of works. Thus the present article is intended to highlight few technological aspects of DRM which are essential in the library profession.

Keywords: Digital Rights Management, Copyright, Rights Expression Language.

1. Introduction

Libraries are increasingly being called upon to provide access to information for citizens in the information society; for e-learning and lifelong learning, to combat social exclusion, to encourage new forms of civic government, to support business and the economy, to help bridge the digital divide. The success of the information society depends on the content being accessible to the public. The Internet and personal computers have changed the way digital media content, such as music, films, books, documents are produced, distributed and consumed. Downloading encoded files has gained acceptance among Internet users because it provides immediate access to content and does not require any physical media such as CD or DVD.

2. Conceptual analysis of Digital Rights Management (DRM)

Digital Rights Management (DRM) means different things to different people. Normally it either means the digital management of rights, as in the context of this paper, or the management of digital rights. The latter term, which is a market enabling technology, encompasses the identification and description of content and includes information about the rights and permissions associated with that content. Usually this is done in such a way as to be interoperable with other content and access systems.

2.1 Digital Rights Management (DRM) is the "transformer" of the Information Age. What started out as software technology used to identify, secure, manage, track, and audit digital content has become a monster of conflicting economic and public policies? It now comes complete with voice raising opponents, lawsuits, business failures and lots of consumer confusion.

2.2 DRM is not only a hot topic; it's also a hot-button issue for the music and film businesses as well as the software developers who created free peer-to-peer (P2P) technologies.

2.3 DRM, also sometimes called Electronic copyright management systems, ECMs, are technologies designed to automatically manage rights in relation to information. This can include preventing copyright works and other information from being accessed or copied without authorization and establishing and enforcing license terms with individuals.

2.4 DRM is a form of continual protection that protects works and manages rights at all times, no matter where the works are located or who has possession of them. DRM attempts to promote authorized use of a copyright work, in part by precluding the possibility of copyright infringement. DRM systems comprise a number of technological components, which can include encryption, a surveillance mechanism, databases of works, owners and users, license management functionality and technological protection measures (TPMs).

2.5 Digital Rights Management (DRM) technology has emerged to protect and manage the intellectual property ownership, commerce and privacy rights of digital content creators and owners as their content travels through the value chain from creator to distributor to consumer, and from one user to another.

2.6 DRM enables greater control over access, use and distribution of content. In an enterprise setting, it can be considered as a security technology, complimentary to firewalls and access control systems, which allows increased control of sensitive, confidential, private or proprietary information.

2.7 DRM enables policy based management for shareable content, controlling access and management of the company's information after its receipt based on well defined policies.

2.8 For a library, a Digital Rights Management system should enable efficient management and rights clearance and It includes the following elements: Digital Rights Management, management of digital rights, contract management, access management, management of the clearance process.

2.9 Digital Rights Management (DRM) can provide the means to control and track the distribution and post-receipt activity of sensitive documents and media. For example, it can be used to protect highly sensitive financial documents, memos and e-mails from being accessed by anyone other than intended management recipients.

2.10 Digital Rights Management (DRM) is known as "Digital Restrictions Management," "Despicable Rights Meddling" or even "Delirious Righteous Morons". by some, the technology and its controversial application of controlling digital content has sparked an escalating battle over copyright protection and fair use.

Thus it is a technology that allows copyright owners to regulate and manage their content when it is disseminated in a digital format, and it's the reason for which some patrons cannot access some of the downloadable digital content that libraries provide.

3. Why are copyright owners interested in DRM?

New technological advances such as the Internet can make it easier to copy and distribute digital works. Potentially, these advances could greatly reduce copyright owners' costs of distributing copyright works. However, some copyright owners

are reluctant to disseminate digital works because they are afraid that their copyright works will be immediately and widely infringed. This is where DRM comes in. DRM promises copyright owners a high degree of control over how works are accessed and used, even after the works are disseminated to users. Thus, copyright owners are interested in DRM because it will help them reduce online copyright infringement. However, there are additional motivations for copyright owners to distribute DRM-protected works. For example, DRM can potentially allow copyright owners to require users to pay for each access and use of a work they wish to make. DRM also possesses the ability to observe and report on usage characteristics, which can provide the distributor of the DRM with unique marketing information not otherwise available. This could give rise to new business models and to a continual revenue stream derived from copyright works. Note, however, that there is no essential connection between DRM and copyright: DRM may be deployed in respect of any content, regardless of the copyright status of the content (i.e., public domain materials are not subject to copyright), and may report to persons other than the copyright owner.

4. Objectives of the paper

The objectives of this paper are to present some key issues to support discussion and articulation of Digital Rights Management (DRM) requirement for academic libraries. The present study is meant to focus the following view points such as

- to know the key concepts and components of Digital Rights Management (DRM),
- to know the key perspectives of DRM,
- to analyze the requirements of Rights Expression Language,
- to focus the role of Librarians for DRM,
- to know the components of DRM.

5. Key components of DRM

The key DRM concepts and components include:

5.1 Rights Data Dictionary: A collection of standardized data elements required to identify entities and relationships in a right's transaction includes the rights or permissions to users (i) for consumption of resource (ii) the constraints on the exercise of those rights (iii) the agents involved in a transactions such as rights of the holder, the user, or the distributors (iv) the application processing the resource (v) the storage device housing the resource.

5.2 Rights Expression Language (REL): A REL communicates rights, obligations, and pertinent information, including identification of entities of participating in a right's transaction. In addition, a REL facilitating and documenting rights transaction among entities, is standardized according to documented rules, and employs a rights data dictionary and a standard syntax, such as XML.

5.3 Right: Parrot (2001) states a right or permission is the most that one can do with a resource. It specifies how one may access or utilize a resource. Guo (2001) describes that the expressions of these rights can quickly become very complex. However, it is critical to understand the expressiveness of the rights in computer language, as the rights model is at the heart of any Digital Rights Management System. Rosenblatt et al. (2001) illustrates the three main rights granted to a user for a certain type of content: render, transport, and derivative rights. **Render rights** include the rights to print, view and play; **Transport rights** include those related to copying, moving or loaning the digital content from one person, place or device to

another. **Derivative rights** include those related to extracting, editing, or embedding the content. All kind of manipulations of digital content are covered. Rosenblatt et al. (2001) states that, there is another right: the right to make a backup copy of content, or the utility right. This includes backup rights, caching and data integrity rights. **Backup rights** allow a copy of the content to be made for the sole purpose of restoring the primary copy if something happens to it. **Caching rights** permit items such as database caches and proxy servers to make local copies of content to improve system performance. **Data integrity rights** include the right given to users to create error-correction codes and other low-level means of ensuring that, data is not corrupted.

5.4 Constraints: Parrot (2001) views that a constraint or obligation is the least on need to do, in order to be granted the right to access or use a resource. A constraint limits or imposes a requirement that must be met to exercise a right.

6. Models of DRM

DRM models are mostly addressing functional, transactional and architectural point of views.

6.1 Functional models describe the main functions provided by DRM. It mainly covers three aspects: the management of rights, the management of the usage, and the management of the content. Management of rights defines the constraints, the granting, and the commercial conditions attached to content. Management of usage enforces the conditions defined by the provider as the usage rights, whereas the management of the content handles the content itself. Thus functional models define concepts such as usage rights management, content packaging and delivery, monitoring.

6.2 Transactional models describe the dynamic behavior for the different steps starting from the packaging of the content and ending to the actual consumption of the protected content. Transactional model puts the focus on the process and its enforcement.

6.3 Architectural models describe the different elements of the architecture of a DRM and their interaction. It mainly deals with servers, services and agents. It identifies the technical services to provide and entities that provide those services. It maps the functional model into corresponding software and hardware elements. This is the most known type of model. Often descriptions of DRM rely on architectural model.

7. Key perspectives of DRM

There are five different key perspectives which give an overall view on Digital Right Management (i) intentional perspective, (ii) functional perspective, (iii) economic perspective, (iv) social perspective, (v) Technical perspective.

7.1 Intentional perspective

7.1.1 The primary intention of a DRM system is to protect the property rights of an enterprise's assets. Another

intention is to establish the awareness of Intellectual Property Rights(IPR) in society. The law influences the digital rights management system with respect to compliance, investigation and enforcement mechanisms.

7.1.2 To create public awareness of intellectual property

7.1.3 DRM for Commerce: This is the use of DRM to protect the monetary value of digital content by protecting it from unauthorized use and enforcing payment terms and conditions associated with its authorized, rightful use.

7.1.4 DRM for confidentiality: This is also known as DRM for privacy, and is the use of DRM to protect confidentiality of information, protect it from unauthorized use, to govern the way it may be used on an authorized basis, and possibly to record when and how it is used. This typically applies to the enterprise, and includes notions of policy management.

7.2 Functional perspectives

It describes the functionalities of DRM system, e.g. protection, management and monitoring of property rights, enforcement of terms and conditions, creation and management of contracts, revenue stream control. There are eight typical functionalities supported by the following six DRM systems such as : Microsoft windows media rights manager; Inter trust rights Manager; Adobe content server; Real networks Real System Media commerce suite; IBM Electronic Media Management System(EMMS); Sun one(open net enterprise);

Typical DRM functionalities are:

7.2.1 Content provision: Content Provision means making the digital content available to the DRM system. This can be achieved by uploading the digital files.

7.2.2 Content administration: This functionality refers to storing the digital content.

7.2.3 Offer creation: Offer creation deals with specifying terms and conditions for a product purchase. Usually this is done by generating licenses with different rights sets. The customer can then choose that kind of license which suits him best.

7.2.4 Content preparation: Content preparation means bringing the content in a secure tradable format. Often content is encrypted and enriched with metadata.

7.2.5 Content Distribution: Digital content has to be made available to customers. Therefore a DRM system should have the ability to integrate e-commerce sites of online retailers, where customers can browse for certain content. Many DRM systems also support super distribution. Thereby people can send digital content from their PCs and portable devices to their friend's PCs and portable devices.

7.2.6 Contract Creation: The functionality "contract creation" means that a customer can purchase, rent, play, etc. digital contract. Thus a contractual relationship between the content provider and the customer is created.

7.2.7 Payment: The DRM system has to provide an interface to a payment systems that can pay for used, purchased services.

7.2.8 Content consumption: Customer needs a special software to support the necessary decryption process and be able to read the rights stipulated in the license.

7.3 Economic perspective

In the view of Guth (2006), the economical factor in DRM include business model and market environment. The tools of digital rights management

don't define how commerce must be conducted rather they allow the business models to be defined, support and their implementation.

7.4 Social perspective

It highlights social, personal and psychological aspects of DRM system. It focuses on the need and willingness of users to use platforms with Digital Rights Management. It addresses social, personal and psychological aspects. It puts questions like why should client use a DRM platform? Why should use DRM platform for downloading instead of using free anonymous source? Microsoft 2002 comments digital distribution offers consumer a convenient way to access the favorite content at any time. The DRM licensing scheme protects consumes in advertently pirating a file: consumers can be confident that digital media they received is the authentic material, and that they have acquired it in a legitimate manner. This DRM aspect can be applied to the six DRM systems to the same extent.

7.5 Technical perspective

It has a number of sub –areas. It covers data model, the secure electronic environment, the system architecture, the applied standards, the protocol stack, the authentication and identification of mechanisms and the digital right languages.

8. Application of DRM by different personalities

8.1 Corporate librarian identifies and locates a key article on a subscriber's site that the organization's head wants to present to the board of directors. Printouts or photocopies will not be suitable; instead, he/she wants professional reprints. The corporate policy also requires one to keep a license on file for this use of the content. Fortunately, this publisher provides the option one need right on its web page. At the bottom of the article, one, spot, the permissions hyperlink; it takes to the DRM system they have chosen. One check the cost and elect to have the PDF version created on the file.. Next one either print the PDF oneself or one opt to forward the document to a printer for high quality printing on a glossy paper.

8.2 Content Manager for the company's intranet. One has been working with one's human resources department and have identified several key chapters from a text book on diversity training, which is about to be introduced to all employees. Using the DRM system on the CD-Rom that accompanies the text book, one is able to obtain a license that unlocks the digital versions of the chapters for oneself, and one post a clean and cleared version of the key chapters on one's intranet site within minutes.

8.3 As a **project leader**, the librarian is asked to redistribute an important and expensive market research report. Time is critical, but the language of the license for the report specifically disallows photocopying. The DRM system, hosted at the publisher's web site, provides him with an electronic copy as well as the permission to distribute it, via e-mail, to other project team members.

9. Role of librarians in DRM Environment

In case of adopting Digital reading materials, the librarians are to be oriented in different level of DRM such as: knowledge on operation control model, knowledge on commercial value control model,

knowledge on content control model, knowledge on compatibility, knowledge on business criteria, knowledge on impart of users.

9.1 Knowledge on Operational control model: It provides knowledge on general issues on DRM as per security and infrastructure technology. Librarian must have the knowledge on following aspects.

9.1.1 Knowledge on software and its application.

9.1.2 Does the organization have the requisite skills to integrate, manage and maintain the DRM system? Is it a core competency? If it isn't, can the skills be learned or acquired? Otherwise outsourcing to a DRM service provider or a professional services organization with DRM experience for the implementation can be done.

9.1.3 Does the organization have the budget to install the DRM system? What is the total cost of ownership (TCO) for the DRM system?

9.1.4 Does the DRM system fit the needs? Does a hosted service offer additional services that more cost effectively fit the needs of the organization? Is customer development program is required to fit the needs?

9.1.5 Does the organization has high enough levels of content delivery or sharing that allow authorization of overall DRM system costs?

9.1.6 How is digital content be delivered? Is it to be delivered on physical media (e.g., CD-ROM) or over a network?

9.1.7 What is the time horizon for the implementation of DRM?

9.1.8 Does the DRM system allow a organization to make a smooth transition from an outsourced or hosted service to an internally managed one?

9.2 Knowledge on Commercial Value control model

9.2.1 DRM protects the privacy or commercial value of digital intellectual property. Critical to that is whether the DRM technology is secure, reliable, scalable and widely deployed.

9.2.2 Are standards-based cryptography algorithms (AES, DES, RSA and SHA-1, etc.) or proprietary algorithms being used? How strong are they? Can they be upgraded and replaced over time in case they are defeated? Can the DRM software on the devices or PCs be updated as well?

9.2.3 How are keys managed, distributed, authenticated, revoked and renewed? Can renewal be done without human intervention? What kinds of revocation are supported?

9.2.4 What is the scope of the damage if a key is compromised?

9.2.5 What tamper-resistance mechanisms exist?

9.2.6 Does the DRM system scale up to handle large numbers of users, pieces of content and devices? Can it scale up in modular increments or does it require a whole new system? What is the architecture being used? Is it peer-to-peer or client-server? Which components are needed to achieve the required scale? ;

9.2.7 Does the DRM system provide consistent capabilities across supported media types? Can it be extended to support other media types?

9.3 Knowledge on Content control model

Content comes in a variety of types (video, audio, text, images) and in a variety of formats. As such it may need to be streamed, delivered as a file, or as physical media such as a CD or DVD. Depending on the company or application, it could be delivered to and accessible from a variety of devices, such as PCs, PDAs or mobile phones, which all run different operating systems.

Furthermore, a company may need to support multiple consumer and non-consumer business models for the delivery of content. Depending on the needs of the application, the following criteria may apply:

9.3.1 Does the DRM work with all the kinds of content needed by the applications (e.g., documents, audio and video)?

9.3.2 Is the DRM available across the range of devices and operating systems (e.g., PC, handheld and wireless mobile phone)?

9.3.3 Does the DRM work with multiple file formats and codes (MP3, REAL, Microsoft, PDF, etc.)?

9.3.4 Does the DRM system support open codes, or does it require the use of proprietary codes? How important is that to the company?

9.3.5 Can it be used to control access to content delivered on physical media or any other distribution method (CD-ROM, DVD and Flash memory, for example)?

9.3.6 Can the current and future range of required business models, expressed in rights and rules, be represented and implemented?

9.3.7 Can additional applications be built using the DRM or is it restricted in its application or focus, such as music only or document only)?;

9.3.8 How does the DRM system handle content sent between users in different organizations? What is required to do that? ;

In general, those criteria are more important for service providers or content owners that aim to build commerce-oriented businesses. They can be equally important to enterprises whose needs for sharing protected content may evolve over time.

That in order to enjoy some of those flexibility benefits, a DRM customer might need to spend time and money to tailor a DRM system to its application needs, technical infrastructure and business goals.

9.4. Knowledge on Compatibility

DRM is an important content security technology, but it cannot function alone. To fully protect content, it must integrate with existing network infrastructures, both within a company and potentially with a partner's systems in the content value chain. Those include:

- Web servers and portals,
- Database and content repositories,
- ERP systems,
- **A**uthorization and directory services,
- **E**-mail systems, and
- **C**ommerce and billing systems (for commercial content).

Standards also play a role in ensuring compatibility, enabling integration and facilitating widespread adoption across the value chain. While proprietary approaches are typical for products in an emerging market, DRM systems must embrace emerging standards for securing content (such encryption

standards as AES, DES and RSA), defining rights and business rules (rights specification languages such as OeBF, XrML and XMCL), content identification (for example, DOI), describing what is contained within an encrypted file (metadata) and industry standards (OMA for use of DRM on mobile devices).

Furthermore, the DRM should be able to work with tamper-resistant, feature-disabling capabilities supported in standard formats and viewers (PDF, for instance). Therefore, compatibility criteria include the following:

- Does the DRM system easily integrate with organization's existing infrastructure?
- Does the DRM system have an open architecture and APIs? Does the DRM support standards that enable interoperability and integration with required systems, such as databases, e-commerce systems or asset management systems (such as XML and ODBC)?
- How much effort, time and cost will the integration entail?
- What are the system requirements for the client and server products (operating system, hardware platform and third-party software)? Does it enable expansion to new hardware platforms and software systems as needs and infrastructures change?
- If the DRM system supports policy-based packaging of content, how easy is it to define new policies or work with existing systems (for example, LDAP or Active Directory)?
- Does it support the company's required file formats and content types? Can the DRM work with feature-disabling capabilities supported in standard formats and viewers (PDF) to further protect the content?
- Does the DRM support the required standards (e.g., content standards, communication standards and security standards)?

9.5 Knowledge on Business criteria

DRM is an emerging market. Like the early days of the Internet security market, a number of companies offer products, some of which may be small, but have very good

technology. Business criteria are equally important when considering the selection of a DRM vendor. The following are some suggested criteria:

9.5.1 Vendor viability: How has the company performed historically? A DRM provider's healthy corporate performance suggests good management and longevity, both of which are essential for delivering ongoing technical support to a DRM customer as its business grows and changes.

9.5.2 Trust and control: Does one trust the DRM system vendor and its products to implement ones business policies and models, and give one the control one want? Does one trust the vendor to hold cryptographic keys to one information or have access to one your transactional data? A DRM system deals with encrypting content and information and is typically integrated at an infrastructure level in an organization. Given this, trust in the vendor is essential.

9.5.3 Price: How much does it cost to implement a DRM system? The total cost to acquire a DRM platform will include purchase, implementation and maintenance costs. Those costs should be carefully considered in terms of potential gains from implementing a DRM system or potential losses from not

implementing it, such as lost revenues, market cap (stock price), and competitive advantage, time to market or reputation. Note that while a low-cost system may fit a company's current needs, it may not scale as the business grows, and may actually necessitate the purchase of an entirely new system at a later date. Conversely, a high-cost system may include extra features that a company does not need.

9.5.4 Return on investment: How substantial will the ROI be on a DRM platform, and how long will it take to recoup it? A company should consider not only whether there will be a return on its investment in a DRM platform but also the time frame in which its investment will be recouped. Since DRM is one component of a larger system, the ROI of the system must be evaluated, as well as that of the DRM.

9.6 Knowledge on Impact on the user

Digital rights management (DRM) is ultimately experienced by a user who is either protecting a piece of

content or attempting to access, render or transfer a piece of content. Depending on whether the organization is using DRM for commerce or for privacy, the criteria for the user impact will be different. Both criteria have consequences to the organization and its business goals:

- Is the packaging of content easy to do or transparent to the user?
- Can it be done automatically on the user's behalf?
- Is the DRM transparent and easy to use (what user interface is shown)?
- What software is required on the client? How is it deployed to the client? Does it require a download? Does it work within a browser?
- How is the client or user authenticated? Is it reasonably transparent? Is it trustworthy? How is it implemented and what does it require from the user?
- What extra steps, if any, does the user need to take to access or view protected content (e.g., download extra files or click on dialog boxes)?
- How does the client enforce rights, rules and permissions?
- Does the DRM system enable portability of content? What devices are supported?
- How is the client software distributed (built into the operating system or applications or distributed from the vendor's Web site)?
- What does the user need in order to view protected content (a special viewer or a standard application)?
- Is the DRM easy to use and easy to teach how to use?
- In all uses of DRM, it is important that the DRM system balances DRM transparency with security, making the DRM transparent and unobtrusive in normal use and appropriately visible when a rule violation occurs.

10. Demerits of Digital Rights Management

The demerits may be categorized into three types.

10.1 Device compatibility

Libraries should always provide content that offers device compatibility for all users. In other words, it shouldn't matter what device one choose to buy, the library's content

should always work on it. Libraries are now being criticized for purchasing content (e-books, video, and music) that's only accessible on devices installed with Microsoft software. But no provider that sells to libraries offers a collection of downloadable audio books, video, or music that works with Apple products.

10.2 DRM Roadblocks

DRM presents a hurdle for library users. For one, DRM-protected content often requires multiple steps to access, as well as the installation of new software, updating of licenses, and new accounts and passwords. The auto-expiration of DRM-protected content for libraries (e.g., after a three-week check-out period) can malfunction and shut out a user who is entitled to full access. Inconsistent terms of use for digital versus print library materials also frustrate library users.

10.3 Archival Issues

E-content that is protected by a "key," a particular device or piece of software necessary to access it is also problematic. The key can be lost or the device may become obsolete. Then the software may not run, because the compatible device no longer exists. These long-term archival issues will affect all libraries. At the speed with which technology changes, material created today may become inaccessible in a decade.

11. Suggestions

- The success of information society depends on digital content being accessible. Digital content must not locked up behind technical barriers.
- Libraries must not be prevented by DRM from availing themselves of their lawful rights under national copyright law and must be able to extend their services to the digital environment.
- Long term preservation and archiving, essential to preserving cultural identities, maintaining diversity of peoples, languages and cultures and in shaping the future must not be jeopardized by DRM.

12. Conclusion

A digital rights management system is a means of delivering content. How ever, DRMS are frequently seen only as a Technical Protection Measure. i.e. a technical means of enabling right holders to deliver digital content in a controlled way, preventing users from having access to the content unless they met the requirements of the right holder, be it financial or otherwise, and preventing users from using the accessed content in ways other than the right holder has given permission for.

Libraries are already involved in the clearance and management of rights. A property managed introduction of Digital Rights Management systems, in its widest sense, could assist libraries in managing their services. However, a restrictive definition of a Digital Rights Management system, which focuses on protection rather than management, may hinder libraries in managing access to their services. Hence a logical, reasonable, easy and easier and faster information access.

References

1. **Becker, Ebehard.** Digital Rights Management-Technological, Economic, Legal and Political aspects. An compendium, 2005.
2. **Bechtold, S Vom.** Urheberzum Informationsr-echt, Implikationen des Digital Rights Management. Verlag C.H Beck HG Munchen, 2002.

3. **Consumer's Guide to DRM** (http://www.indicare. org/tiki-page.php?page=consumer guide

4. **Einhorn, M.** Digital Rights Management and Access Protections: an Economic Analysis In: Ginsburg, J. et al.(eds,) Adjuncts and Alternatives to Copyright, Copy Co Printing, New York, 2002, pp. 1234 -1240

5. **Gordon, L.** The Internet Marketplace and Digital Rights Management. In Digital Rights Management: Concepts and Applications, edited by S Kambhammettu. Le Magnus university Press, Hyderabad, 2005 pp,103-122

6. **Guo, H**. Digital Rights Management (DRM) using XrML URL: http://www.tml..hut.fit/studies/T-110.501/2001/papers/guo.heng.pdf. 2001

7. **Guth, S**. Interoperability of DRM systems: via the exchange of Xml-based Rights Expressions, Peter Long Pub Inc, 2006.

8. **Guth, S And Iannella, R.** Open digital rights language(ODRL) version 2 requirements, Feb 2005; http://odrl.net/2.0/v2 req: html

9. **Hauser, T. And Wenz, C.** DRM under attack: Weakness in Existing Systems. In Digital Rights Management – Technological, Economic, Legal and Political Aspects, edited by E Becker et al. Berlin: Springer, 2003, pp. 342-362

10. **Iannella. Renato.** Digital Rights Management (DRM) Architectures, D-Lib Magazine, 2001, 7(6), URL:http//www.dlib.org/dlib/june01.iannella/06iannella.html, (accessed:2005-07-01)

11. **Lawrence, Lessig.** Free culture. Basic books, 2004(http://free-culture.org/freecontent/). 2004.

12. **Parrot, David.** Responding on behalf of Reuters. Requirements for a Rights Data Dictionary and Rights Expression Language. MPEG-21, March 2001.

13. **Rsenblatt, B., Trippe, B and Mooney, S,** Digital Rights Management-Business and Technology. M and T Books, New York, 2001.

14. **Rump, N.** Digital Rights Management: Technological Aspects, In: Becker e. et al (eds.) Digital Rights Management – Technological, economic, Legal and political Aspects, Springer, Berlin, 2003 pp-3-15

15. **Slowinski, H.** What Consumers Want in Digital Rights Management (DRM): Making Content as Widely Available as Possible in Ways that Satisfy Consumer Preference. In: Kambhammettu S.(ed.) Digital Rights Management : Concepts and Applications, Le Magnus university Press, Hyderabad, 2005. pp.175 – 190.

About Authors

Dr. (Mrs) Puspanjali Jena, Reader,
Department of Library and Information Sciences,
Utkal University, Vanivihar, Orissa.

Mr. Dipak Kumar Khuntia, Librarian cum Documentation Officer,
Xavier Institute of Management, Bhubaneswar.
E-mail : deepak@ximb.ac.in