DIGITAL RIGHTS MANAGEMENT SOLUTIONS FOR ENTERPRIZES: AN OVERVIEW

[PAPER ID: ICITER-C111]
PROF. TODMAL SATISH R
JSPM Imperial College of Engineering& Research, Pune, India
srtodmal@gmail.com

DR. SUHAS H PATIL
Bharati Vidyapeeth University College of Engineering, Pune, India
suhas_patil@yahoo.com

ABSTRACT:

In 21st century the digitalization of the processes and information has taken place very rapidly. Every organization in the competitive era has the confidential information and processes. The success of every organization is based on the security of such secret data and information.Confidential data, information, processes plays a vital role in development of the enterprise, in order to withstand in this market with a huge business competitors. Security of such information is really a challenge and many researchers have tried addressing this problem in last decade.Theft of such data may include the product development information, research data, business plans, financial details, list of the customers. It has been observed in the research that most of the times such data is stolen by insiders. Authors have tried to present the overview of various solutions proposed by researchers in past decade.

KEYWORDS: Digital Rights Management, Information Theft, Rights management systems.

INTRODUCTION:

The internet users are increasing very rapidly, as the world is progressing towards digitalization. Up till now approximately 46.1% of world population has internet accessas that of less than 1% in 1995 [1]. As the use of internet has increased rapidly, most of the important information and records are also converted in digital form. The digital information has several advantages whereas security of such data is also a big challenge as it has easy access.Therefore, the digital rights management is really important to avoid the theft of such data.

Every enterprise is preparing, storing and sharing the data in digital form nowadays. Most of the times, the data is shared by means of internet in the form of emails. The use of internet has made the handling of data very easy and rapid at the same time the security is less if the person having access to the data has decided to misuse it.If such information is received by any unauthorized person then there is risk of disclosing such important information. The enterprise never affords to disclose any confidential information with any outsider. The outsiders have to take high extra efforts to extract the data from an enterprise, while insiders have easy access to such data. Such insiderattacks are really severe as fur as security of the data is concerned. The economical losses due to information theft are never be neglected as it affects the growth rate of any enterprise. The need of time is to develop the security system without disturbing the working model of the enterprise [2].

REQUIREMENTS OF DIGITAL RIGHTS MANAGEMENT:

Due to the fastest growing digitalization it's really needed to provide the solution for DRM by considering all the aspects and requirement. The DRM system must consist of the following properties-

i. Interoperability
ii. Security
iii. Complexity-efficacy balance
iv. Privacy
v. Transparency
vi. Robustness

A cluster of research is carried out and in the experimentation it was found that the systems those fulfill the above mentioned requirement are as mentioned below.

DIGITAL RIGHTS MANAGEMENT [DRM]:

The digital rights management is the term related to the protection of digital contents. The rights of using such contents are reserved with the original owner of the contents and no one can reuse it without the having rights to reuse. DRM is process of controlling and managing the right to such contents. DRM is mainly classified in to:

1. Controlled distribution of digital contents
2. Enterprise digital rights management (E-DRM)

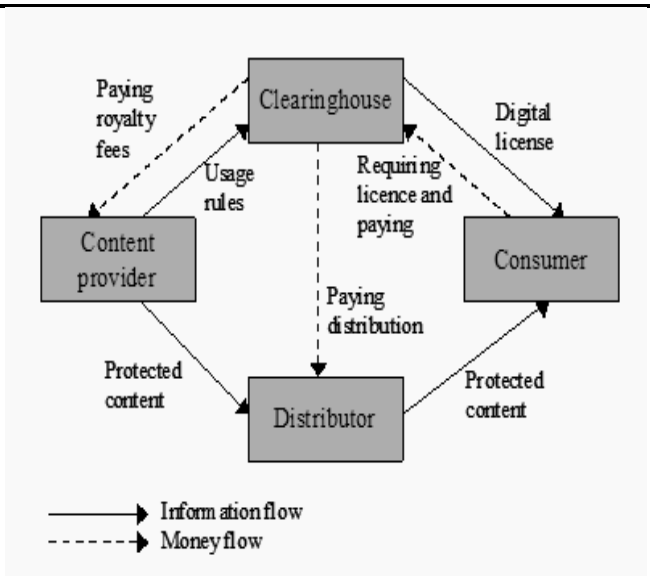


Figure 1: Basic content protection oriented DRM system

The above diagram shows the basic content protection oriented DRM system. Content protection is generally achieved by the digital license identifiers. One can distribute and sale the digital contents with this license safely [3-4].The digital contents are stored in the library called content server, while the license server provides license to use the contents.

OVERVIEW:

Authors are trying to discuss the details of various DRM systems.

i. MICROSOFT WINDOWS RIGHTS MANAGEMENT SERVICES:

Microsoft has adopted the rights management service (RMS), the additional safety is provided to the digital data while working with MicrosoftWindows. The windows RMS service has mainly three components:

1. RMS server software
2. RMS client software
3. RMS-enabled applications

The information stored with the license and one can access it by providing the properlicense. The security strength if the windows RMS system can be challenged by outside attackers, whereas the authorized insiders have full control over the rights of protected contents.

ii. LIQUID MACHINES:

This is another solution to address the problems in E-DRM, with the online and offline access rights. Central repository of the liquid machine server defines right policies for the file to be protected. The user can access the information offline for the stipulated time through NT-LAN Manager. The integration of system is possible with most of working background.

iii. AUTHENTICA'S PAGERECALL:

The rights and keys to use the informationare stored on central server. The information is accessed when the client is connected with the central server as the rights are not dispersed with the protected files itself. Complete control over the information is provided at the server. If the protected files are allowed to work offline feature while assigning the license, once can access it in offline mode too. The license created is stored on the server in the form of PDF file. Sometimes users avoid using the PDF contents; hence it is not one of the popular systems.

iv. DISPLAY-ONLY FILE SERVER (DOFS):

This solution is more effective against insider attacks. The important files are stored on secured server. The user can read or write the files in pdf or word format, but can't make changes in the file. Offline use of the files is also possible by a precise checkout system i.e. tamper-resistant system. Unauthorized insider can't even access these files. Most of the data is in the form of images.

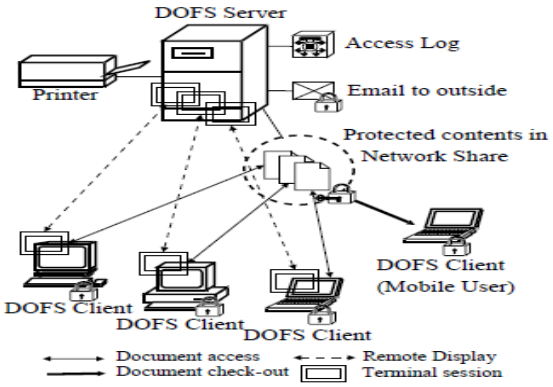


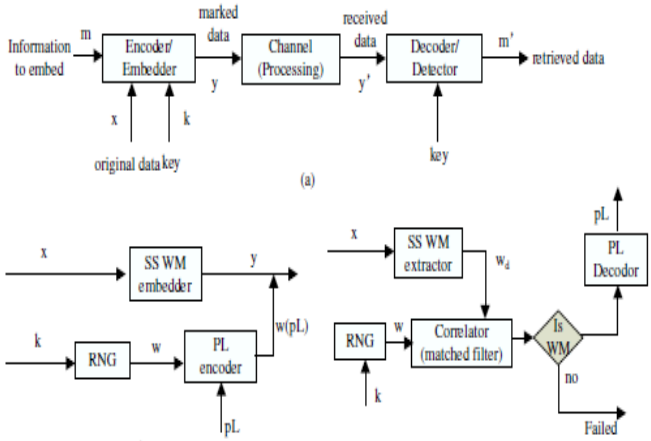
Figure 2: Basic DOFS System [5]

The configuration of the DOFS system is shown in Figure 2, the access to the files is provided to the authorized person. While the others insiders cant access the data. The system is designed such that one can't even email the information while accessing it.

DIGITAL WATERMARKING AND COPYRIGHT INFRINGEMENTTRACING:

Researchers have also proposed the digital watermarking and copyright scheme for the security of the documents. This is a reactive approach for authentications

and copyrights. A basic model of watermarking scheme is shown in the figure below.



The properties required by the watermarking scheme are:

i. Transparency
ii. Robustness
iii. Security and
iv. Capacity

CONCLUSION:

In this paper authors have presented the overview of various digital rights management systems. The need of such system is to secure the digital data against inside and outside attacks. Confidential records and data are vital for every enterprise and theft of such data not only results in the misuse of information but also in economic loss. The basic digital rights management systems were discussed in this paper.

REFERENCES:

i. http://www.internetlivestats.com/
ii. S. H. Kwok, C. C. Yang, and K. Y. Tam, "*Intellectual Property Protection For Electronic Commerce Applications,*" Journal of Electronic Commerce Research, vol. 5 pp. 1-13(2004).
iii. IMPRIMATUR. *Synthesis of the Imprimatur Business Model.*<http://www.icestandard.org>. Accessed on 28.9. 2004.
iv. Liu, Q.; Safavi-Naini, R.; and Sheppard, N.P. *Digital Rights Management for Content Distribution,* In, Johnson, C., Montague, P., and Steketee, C., (eds.).Australasian Information Security Workshop 2003, Adelaine, Australia: Australian Computer Society Inc., 2003, pp. 49-58.
v. Yu, Yang, and Tzi-ckerChiueh. "*Enterprise digital rights management: Solutions against information theft by insiders.*" Research Proficiency Examination (RPE) report TR-169, Department of Computer Science, Stony Brook University (2004).
vi. Bill Rosenblatt, Bill Trippe and Stephen Mooney. *Digital Rights Management: Business and Technology.* M&T Books. 2002
vii. Brian A. LaMacchia. Key Challenges in DRM: *An Industry Perspective. Proceedings of 2002 ACM Workshop on Digital Rights Management.* November 2002.
viii. Computer Security Institute (CSI) and the FBI, 2003 *Computer Crime and Security Survey*. http://www. Security fsu .edu/docs/FBI2003.pdf
ix. David A. Solomon and Mark E. Russinovich. *Inside Microsoft Windows 2000.Third Edition. Microsoft Press.*
x. *Driving the Standard for Interoperability in Digital Rights*. MPEG REL Software Development Kit for Java User's Guide. Content Guard Inc.
xi. *Extensible rights Markup Language* (XrML) 2.0 Specification, Content Guard, Inc. Nov. 2001.
xii. K. Fan, W. Mo, S. Cao, X. Zhao, and Q, Pei, *"Advances in digital rights management technology and application,"* ACTA Electronica Sinica, vol. 35, no.6, pp. 1139-1147, 2007.
xiii. K. Fan, M. Wang, W. Mo, Z. Wang, Q. Pei, and J. Shen, *"An iris biometric-based digital multimedia content protection scheme,"* ACTA Electronic Sinica, vol. 16, no. 2, pp. 271-275, 2007.
xiv. N. Fazio, *On Cryptographic Techniques for Digital Rights Management*, New York University, Sep. 2006.
xv. D. Fewer, P. Gauvin, and A. Cameron, *Digital Rights Management Technologies and Consumer Privacy,* Canada Internet Policy and Public Interest Clinic, 2007. (http://www. Cippic.com/drm)
xvi. E. Furregoni, A. Rangone, F. Renga, and M. Valsecchi, "*The mobile digital contents distribution scenario,"* Proceedings of Sixth International Conference on the Management of Mobile Business, Toronto, Ontario, Canada, pp. 32-40, July 2007.
xvii. Y. Chang, "*Who should own access rights? A game-theoretical approach to striking the optimal balance in the debate over digital rights management,"* Arti- ficial Intelligence and Law, no. 15, pp. 323-356, 2007.
xviii. [17] C. Chong, *Experiments in Rights Control Expression and Enforcement*, University of Twente, Enschede, The Netherlands, 2005.

xix. D. Chong and R. Deng, "*Privacy-enhanced super distribution of layered content with trusted access control,"* Proceedings of 2006 ACM Workshop on Digital Rights Management, Alexandria, Virginia, USA, pp. 37-43, Oct. 2006.

xx. *Content Management License Administrator Technical Report Revision* Ver. 1.2-070326, CMLA: Client Adopter Agreement, Mar. 2007.

xxi. C. Conrado, M. Petkovic, and W. Jonker, "*Privacy preserving digital rights management,"* Proceedings of 2004 SIAM International Conference on Data Mining, LNCS 3178, pp. 83-99, 2004.

xxii. A. Cooper and A. Martin, "*Towards an open, trusted digital rights management platform,"* Proceedings of 2006 ACM Workshop on Digital Rights Management, Alexandria, Virginia, USA, pp. 79-87, Oct. 2006.