IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-2, April 2016 E-ISSN: 2347-2693

Review Of Secure And Privacy Preserving DRM Scheme

Bhavana S. Rote[1], M. M. Deshpande[2]

[1] *Computer Department, Mumbai University, India,*
[2] *Computer Department, Mumbai University, India*

www.ijcseonline.org

Abstract— Digital rights management (DRM) is becoming a key enabling technology to protect intellectual property of digital contents and it controls dissemination and usage of digital content. Numerous researches have been conducted for DRM since the past decade. This paper summarizes the basic concepts in DRM and present the typical DRM reference architecture. Secondly, requirements in this domain are studied. Furthermore, the some existing techniques are presented with detail analysis to point out the advantages and disadvantages respectively.

Keywords— Digital Rights Management (DRM), Interoperability, Proxy Re-encryption, Homomorphic encryption.

I. Introduction

Shifting from traditional content, such as paper documents, to digital media is due to several advantages of digital media over the traditional media. Exact copies of digital data can be easily made. Digital content (audio, video, graphics, and images) can be easily copied, transmitted and distributed over networks. On one hand this represents a very important property, but on the other it also creates a problem as copies cannot be distinguished from the original. This is one of the main factors which hinders the growth of multimedia networked services because it has a negative impact on the willingness of authors, publishers and providers of multimedia data to endorse distribution of their documents in a networked environment. Easy reproduction of digital data in their exact original form is likely to encourage problems such as copyright violation, unauthorized use and abuse. This is perceived by many as a threat to the content value, particularly in the music and movie industries. It prevents digital media publishers from receiving payment for each copy made out of a digital work.

DRM is the important technology of taking a series of measures to protect the digital contents from being abused and make sure that digital contents are fair to use. Digital rights management (DRM) ([3], [7]) is a term referring to various access control technologies that are used to restrict the usage of proprietary software, hardware, or content. DRM includes technologies that control the use, modification, and distribution of copyrighted works, as well as systems within devices that enforce these policies. The term is also sometimes referred to as copy protection, copy prevention, and copy control. Digital Rights Management is important to creators and publishers of electronic media since it helps ensure profits for their products. Typically, a DRM system protects intellectual property by encrypting the data so that it can only be accessed by authorized users. Digital rights management is sometimes referred to as digital restriction management. In general, the purpose of DRM is perceived as a way of preventing people via technological means from using copyrighted material in ways that are unacceptable to the publisher.

Contributions:

We present analysis of various existing DRM schemes with their advantages and disadvantages. We compare different DRM scheme by taking into account following factors: scheme, security, key re-encryption, content re-encryption, traceable system, profile building prevention, privacy and user anonymity.

A. DRM Architecture

There is no standard DRM architecture – there are many different frameworks offered by different vendors. In general, there are four parties in the DRM system architecture, that is, the content provider, the distributor, the license server, the consumer (Fig 1). Further information is as follow:

1) Content Provider: A content provider is an entity that offers the encrypted content and establishes rules and licenses. In general, to protect the digital content, the symmetric or asymmetric cryptosystem is adopted. The main responsibility of content provider is to hold the rights to duplicate or distribute the content.

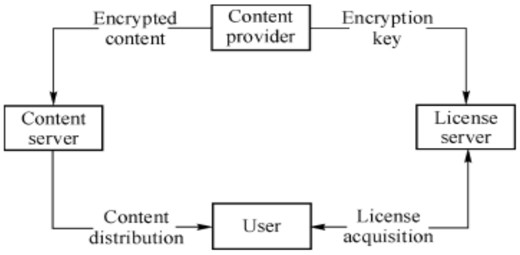

Fig 1: DRM Architecture[10]

2) Distributor: The distributor is an entity that enables the encrypted content available to the consumer. In general, the distributor always sets the encrypted content on its website over the Internet. Therefore, the consumer can connect to the website of the distributor and download the encrypted content.

3) License server: The duty of the license server is to issue the license to consumer and handle the financial transaction data. The license server is responsible for collecting payment from the consumer and portioning out the fee to the content provider and distributor.

4) Consumer: This refers to people who use DRM system to acquire the digital content by downloading from the distributor and purchase license for playing the content.
The remainder of this paper is organized as follows: requirements of DRM scheme is covered in Sect. II. Various DRM schemes are given with their merits and demerits in Sect. III. Finally Section IV provides the concluding remark of the whole paper.

II. REQUIREMENTS

We introduce the following requirements for DRM schemes:

A. Protection

DRM should provide protection of digital content. This type of protection is typically provided by the encrypting technique, which enables authors and publishers to send digital content across an unsecured network, such as the Internet; this way the content can only be read by the intended recipients.

B. Security

The content provider expects that digital content must be encrypted and authorized user must not be able to extract and store the decrypted content, and also content confidentiality against unauthorized users must be achieved.

C. Efficient

User expects to access the content via multiple devices anytime anywhere, and also asks for flexible usage model. Therefore, the DRM scheme should support efficient license models, and have low computational complexity to support massive users.

D. Privacy preserving

Privacy preserving is the protection of personal information. The user should stay anonymous.

III. VARIOUS DRM SCHEME

Digital rights management (DRM) was introduced to protect the copyright of digital contents in digital environments. Various DRM technologies are currently available. In most cases, the use of digital contents on several devices is blocked by digital rights management (DRM) technology to protect the rights of digital content owners, which is called as the DRM's walled garden strategy. This strategy has raised many legal, economical, and ethical problems. One way to complement this strategy is DRM interoperability[3]. Without DRM interoperability, consumers have to repeatedly purchase the same digital contents if they wish to use them on their heterogeneous devices. Consumers frequently criticize content providers because they are generally adopting non interoperable DRM schemes. On the other hand, a recent survey has shown that many consumers are willing to pay more money for contents with interoperability. Therefore, DRM interoperability is required to increase activities in the digital market while protecting the digital copyright.

Many works ([1], [2], [3], [4], [5]) have been focused on the DRM content sharing problem. In general, the key solution for this problem is to translate the DRM content from one format to other formats accessible by other devices. Some solutions [1], [2] require a trusted third party to manage content translation, but these solutions rely too much on the third party. Once the third party is compromised or lost, anyone can use it to translate the content. Some researchers [3], [5] proposed to use proxy re-encryption schemes (PRE) for content sharing ([3],[6]).

Lee et al.[3] proposed a secure mutual-profitable DRM interoperability scheme. The proposed scheme minimizes the disclosure of DRM technology and content providers' security properties by using designated proxy re-encryption and neutral format schemes [4]. The designated proxy re-encryption scheme allows a designated proxy to re-encrypt specific content without revealing the raw content, while the neutral format scheme allows for format independent translations. Taban et al. [5] also used a proxy re-encryption scheme [10] for DRM interoperability. Their scheme, however, cannot designate a proxy to perform the re-encryption and also cannot specify the content to be re-encrypted. Therefore, if someone were able to obtain a re-encryption key from device A to device B, he/she could illegally re-encrypt and deliver all contents of the device A to the device B. In the proposed scheme, however, if someone obtained a re-encryption key, he/she could only be able to re-encrypt specific contents. Therefore, the proposed scheme is more secure than the Taban et al.'s scheme [5].

However, we find this scheme is not secure under a collusion attack: Malicious employees in DRM technology provid (also called DRM server in [3]) and DRM Agent can collude to make copies of a purchased content accessible to any devices without letting content provider know, thus an illegal content sharing could be done bypass content provider. This attack reduces content provider's benefit.

The main problem of existing PRE schemes is failing to provide the non-transferable property. A proxy re-encryption scheme is said to be non-transferable if the proxy and a set of colluding delegatees cannot re-delegate decryption rights to other parties. On one hand, this is a very desirable property. For example, user A saves some encrypted private confidential files on the file server. If A delegates B the decryption right for accessing those files, A may need some guarantee that his files ”go no further”. It requires that the delegatee B plus the proxy cannot re-delegate decryption right to others. On the other hand, researchers are even not sure that transferability can be preventable since the delegate B can always decrypt and forward the plaintext to another party. However, this approach requires that the delegatee remains an active, online participant. What we want to prevent is the delegatee (plus the proxy) providing other parties with a secret value that it can be used offline to decrypt A's ciphertexts. Again, the delegatee can always send its secret key to another party. But in doing so, the delegatee puts itself in a risky situation.

He et al.[6] proposed a novel DRM infrastructure which is based on a non-transferable re-encryption scheme. In the proposed infrastructure, DRM technology providers and content providers are required to cooperate to make a purchased digital content for a specific device accessible by other different devices. The Non-Transferable Pre Scheme used in this paper were proposed in [7]. The main idea of the Non-Transferable Pre Scheme [7] are as follow: Before delegation, delegator will send delegatee's identity to private key generator (PKG). PKG is responsible for generating the re-encryption key, and sending this key and some other information to delegator. Delegator checks the correctness of the re-encryption key and generates a partial decryption key making use of the information received from PKG. Then, delegator sends the re-encryption key to the proxy, and the partial decryption key to delegatee. The proxy re-encrypts the original cipher text from delegator, and sends the re-encrypted cipher text to delegatee. The delegatee can decrypt the cipher text using his private key and the partial decryption key received from delegator. In non-transferable PRE, re-encryption key is generated by a key generating centre (PKG); Delegator participants actively to help generating partial decryption key for delegatee using part of his private key. Thus delegatee and proxy cannot collude to re-delegate decryption rights since they do not have knowledge of PKG's master secret and the delegator's private key. Although these schemes can protect contents well and prevent malicious employees of DRM server from issuing licenses without letting content provider know, they do not consider user privacy.

In order to preserve user privacy in cloud computing, Petrlic et al. [8] proposed a privacy preserving cloud DRM scheme that allows users to stay anonymous and that prevents any party from building user profiles. The proposed scheme extends the proxy re-encryption scheme by Ateniese et al. [9] to achieve indistinguishability of first-level cipher text under the condition that the same second-level cipher text is re-encrypted for the same party more than once. However, this scheme need to re-encrypt the content every time when the user consumes the content.

In contrast to the scheme proposed by Petrlic [8], which is based on proxy re-encryption, Huang et al. [10] propose a secure and privacy-preserving digital rights management (DRM) scheme using Homomorphic encryption in cloud computing. Author present an efficient digital rights management framework in cloud computing, which allows content provider to outsource encrypted contents to centralized content server and allows user to consume contents with the license issued by license server. Further, he provide a secure content key distribution scheme based on Additive Homomorphic Probabilistic Public Key Encryption (AHPE) [11] and Proxy Re-encryption (PRE). The provided scheme prevents malicious employees of license server from issuing the license to unauthorized user without letting other parties know. In addition,this scheme allows users to stay anonymous towards the key server and service provider. This scheme protects the content and privacy without re-encrypting the content. Therefore this scheme has a lower computational complexity and has high efficiency and security.

IV Conclusion

In this paper, we present an importance of Digital Right Management (DRM), architecture of general DRM scheme and requirements of DRM scheme. After that we discussed various DRM schemes by considering their merits and demerits. Table 1 shows comparison of various DRM schemes which we have discussed in this paper by taking into account following factor: security, key re-encryption, content re-encryption, traceable system, profile building prevention, privacy and user anonymity.

TABLE I. COMPARISON OF VARIOUS DRM SCHEMES

Research paper	**Secure**	**Privacy preserving**	**Key re-encryption**	**Content re-encryption**	**Traceable system**	**Profile building prevention**	**User anonymity**
A Secure And Mutual Profitable DRM Interoperability Scheme [3]	NO	NO	YES	NO	YES	NO	NO
Avoid Illegal Encrypted DRM Content Sharing with Non transferable Re-encryption [7]	YES	NO	YES	NO	YES	NO	NO
Proxy Re-encryption in a Privacy Preserving Cloud Computing DRM Scheme [8]	YES	YES	NO	YES	NO	YES	YES
Secure and Privacy Preserving DRM Scheme using Homomorphic encryption in cloud computing [10]	YES	YES	YES	NO	NO	YES	YES

ACKNOWLEDGMENT

We express our profound gratitude to Dr. D.G. Borse (Principal, A.C.Patil College of Engineering), Dr. (Mrs.) Sangita Chaudhari and Prof. (Mrs.) Archna Shirke for their cordial support, valuable information and guidance.

REFERENCES

[1] Durand, M. Eluard, S. Lelievre, and C. Vincent. “Smartpro : A smart card based digital content protection for professional workflow.”In Smart Card Research and Advanced Applications,8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008. Proceedings, Lecture Notes in Computer Science, pages **255– 266**. Springer, **2008**.

[2] D. W. Kravitz and T. S. Messerges. “Achieving media Portability through local content translation and end-to-end right management.”In Proceedings of the Fifth ACM Workshop on Digital Rights Management, Alexandria, VA, USA, November 7, 2005, pages **27– 36**. ACM, **2005**.

[3] S. Lee, H. Park, and J. Kim. “A secure and mutual-profitable drm interoperability scheme”. In Proceedings of the The IEEE symposium on Computers and Communications, ISCC ’10,pages **75–80**,Washington, DC, USA, **2010**. IEEE Computer Society.

[4] Aafa J S and Soja Salim, "Fingerprint Privacy Protection Techniques: A Comparative Study", International Journal of Computer Sciences and Engineering, Volume-02, Issue-07, Page No (86-89), Jul -2014, E-ISSN: 2347-2693

[5] G. Taban, A. A. C´ardenas, and V. D. Gligor. “Towards a secure and interoperable drm architecture”. In Proceedings of the Sixth ACM Workshop on Digital Rights Management, Alexandria, VA, USA,October 30, 2006, pages **69–78**. ACM, **2006**.

[6] He Y J, Hui L C K, Yiu S M. “Avoid illegal encrypted DRM content sharing with non-transferable re-encryption”. Proceedings of the IEEE 13th International Conference on Communication Technology (ICCT’11), Sep 25−28, 2011, Jinan, China. Piscataway, NJ, USA: IEEE, **2011: 703−708.**

[7] Y.-J. He, T. W. Chim, L. C. K. Hui, and S. M. Yiu. “Non-Transferable proxy re-encryption scheme for data dissemination Control”. http://eprint. iacr.org/2010/192.pdf.

[8] Petrlic R. “Proxy re-encryption in a privacy-preserving cloud Computing DRM scheme”. Proceedings of the 4th International Symposium on Cyberspace Safety and Security (CSS’12), Dec 12−13, 2012, Melbourne, Australia. LNCS 7672. Berlin, Germany:Springer-Verlag, **2012: 194−211**

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. **1–30, 2006**.

[10] HUANG Qin-long, MA Zhao-feng, YANG Yi-xian, FU Jing-yi, NIU Xin-xin. “Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing” The Journal of China Universities of Posts and Telecommunications, pages **88–95**, December **2013.**

[11] Rivest R L, Adleman L, Dertouzos M L. “On data banks and privacy homomorphisms. In: Foundations of Secure Computation”. New York, NY, USA: Academic Press, 1978: 169−177

AUTHORS PROFILE

M. M. Deshpande received the M.Tech. degree in the Interdisciplinary programme of systems and control engineering from IIT Bombay, India, in 2003 and Ph.D. degree in system and control engineering from IIT Bombay in 2009. His research interests include image and signal processing and security.

Bhavana Rote is currently pursuing the ME degree in computer engineering from A.C.Patil College of Engineering , Mumbai University,India. Her area of interest is security.