A Brief Review On Digital Rights Management Mechanisms With And Without Trusted Third Party

Authors

Jashoda N. Balla¹, Amol A. Phatak²
PG Scholar¹, Assistant Professor²

Department of Computer Science and Engineering. N.B.Navale Sinhgad College of Engineering, Solapur. Maharashtra-India.
Email- jashodaballa@gmail.com

ABSTRACT

The mechanism of Digital Rights Management is growing it popularity nowadays. There are many subareas in this domain to be handled. Maintaining the security of the digital contents without compromising the privacy of the entities is one of the major requirements. Achieving accountability along with privacy at the same time in same framework is a difficult task. These attributes are mutually contradictory to each other. Hence, there are trusted third parties used for providing privacy to the entities. But what if these third parties are malicious. There are other systems that use other methods for providing privacy instead of using third parties. We have reviewed various scenarios related to digital right management technique.

Keywords—Digital Rights Management, Trusted third party, Accountability, Privacy.

I. INTRODUCTION

In our day to day life the use of digital content has increased greatly because of the quality provided is high and efficient in storage distribution. There are many forms of digital contents like text, audio, video, graphic images and pdf documents. Information available for distribution among several users via electronic media is called as digital contents [1]. Example of digital contents is ebooks or iTune songs, etc. These digital contents are provided with some rights and the management of these rights is done by Digital Rights Management mechanisms. The digital contents are used by customers/users around the world. DRM creates a digital trading platform for users and customers. Following figure 1, illustrates the fact how the customers access the digital contents.
There are many improvements in digital rights management system over a period of time because of varying changes in copyright violation of digital contents. The different generations of the digital rights management systems intended to control different malicious practices that preconceived to use the digital contents. The first generation DRM system aimed to control copying. The second generation DRM software’s intended to control viewing, copying, printing and altering of works or devices.

The advanced DRM systems succeeded in controlling the copyright violation of digital contents. This has resulted in the violation of the privacy of the entities involved. The DRM systems must provide accountability in which the distributor or user must be accountable for the misuse of the contents or licenses purchased by them. Accountability will make sure that the users or distributors be careful and knowledgeable in using the content as even slight negligence can cause them to be legally responsible.

Accountability and privacy need to be achieved together within the same framework. This was achieved with the help of a trusted third party (TTP). However, a trusted third party can also become malicious and break the privacy of the involved entities. Thus both these attributes need to be achieved without the use of a third party. We consider both these scenario in this paper.

During this review, we present the Digital Right Management without trusted third party in section II. In section III, we briefly review the Digital right management with trusted third party and in section IV we describe the summary of the review paper.

II. DIGITAL RIGHTS MANAGEMENT SCENARIO WITHOUT THIRD PARTY

A good survey has been done on privacy preserving mechanisms proposed for digital right management [2, 3]. But the consideration of accountability and privacy has not been discussed yet. Attaining both i.e. accountability and privacy at the same time is a very difficult task, because these two properties are mutually contradictory to each other [4]. Systems that try to achieve accountability and privacy at the same time are
considered to use a trusted third party. But this is unappealing because the users of the system cannot be sure whether the third party is genuinely trustworthy. This may create a problem for user’s privacy.

In a DRM system, there are two types of users: first is the content owner and second is the content consumer/customer. Generally, DRM focuses on protecting the intellectual property of the content owners, but defocus on the protection of the consumer’s privacy. This concern is handled by the authors M. Feng & B. Zhu in [2]. They have proposed a system with DRM mechanism and protect the consumer’s privacy while acquiring the licence. The licence server creates a decryption key of a specific content and then gives the key to the consumer with the licence. The encryption of the content with the encryption key, remains unknown. This proposed work is carried out with the help of blind signature primitive in licence acquisition protocol. Also a different key scheme is used, where the encryption key is a generated with a combination of secret key (only known to the licence server) and information related to the content object.

Another method for protecting user’s privacy has been proposed in [5]. The author has discussed a cryptographic notion called as blind decoding. Blind decoding is a very convenient tool used for protecting user’s privacy. It is applied while using online shopping sites. In this process, the client encrypts the content with the server’s public key and then sends the content to the server. On receiving the content, the server decodes the contents and keeps the decoded contents and it’s private key secret. The author has added a new work to the existing one, by using ElGamal encryption scheme.

A very strong license acquisition and usage tracking scheme has been proposed in [6]. The scheme known as License Management Scheme with Anonymous Trust (LMSAT) has been proposed. It gives freedom to the user to access the contents or data at anytime and from anywhere without disclosing its identity. The system make use of the Elliptic Curve Diffie Hellman key agreement scheme, establishing a secure communication channel. The system also protects the user against malicious attackers.

An effectual and vital scheme has been proposed in [7]. The scheme is called as k-times anonymous authentication scheme, where the time and space complexities are constant at the cost of O(k) sized public key. There are also other anonymous authentication systems like k-TAA, where proper cryptographic primitives are used for securing applications.

A system that is proposed in [8], uses an anonymous token set for facilitating privacy and accountability without third party in a same framework. The user gets a set of l anonymous tokens from the owner and then uses these tokens for purchasing the contents. The tokens are also useful for detecting the malicious users if any and provide privacy and protection against the user. Also the proposed system provides access control policy without compromising the user’s privacy.

III. DIGITAL RIGHTS MANAGEMENT SCENARIO WITH THIRD PARTY

Privacy conserving Digital Rights Management schemes that makes use of trusted third party have been briefly discussed in [9, 10, 11, 12]. In [12] the authors have proposed a mechanism using anonymity ID for
providing privacy in DRM. For retrieving anonymity ID the user needs to certify the authentication server. The authentication server links all the anonymity IDs with the user’s identity. This problem has been addressed in [9] and [11] by separating the responsibilities between certification authorities and content providers. In order to abrogate the users from further use, the third party needs to amalgamate the anonymity ID with the real identity of user. This debilitates the privacy protection of the users, because the third parties can intrigue with an innocent user. In [10], cryptographic primitives such as “verifiable secret sharing,” “zero knowledge proofs,” and “time capsule” have been used to design a privacy preserving scheme for DRM.

IV. CONCLUSION

For withstanding the privacy needs, Digital Rights Management (DRM) is considered to be the best possible way. But the technological properties of DRM are not so supportive. Due to the lack of consideration of user’s privacy, the DRM is gradually failing. In order to improve the rights protection capability, DRM has to supply an unbiased protection to the user’s privacy and placate the provider’s rights. DRM system will be successful if the tension between the users and content providers is diminished; that is, if piracy is controlled, fair use is implemented and privacy is protected. We have proposed a unique privacy empowered digital rights management mechanism eliminating the use of trusted third party.

REFERENCES

6. S.Nair, Bogdan C. Popescu, C. Gamage, B. Crispo, A. Tanenbaum “Enabling DRM-preserving Digital Content Redistribution” Dept. of Computer Science

