DIGITAL RIGHTS MANAGEMENT - CURRENT STATUS AND FUTURE TRENDS

Hisham Abdalla, Xiong Hu, Abubaker Wahaballa, Ahmed Abdalla, Mohammed Ramadan, Qin Zhiguang
School of Computer Science and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-mail: hisham_awaw@hotmail.com

Abstract- In this paper, a taxonomy of privacy-preserving approaches employed in digital right management systems are presented. These approaches are classified into two main approaches according to their design philosophy: cryptographic and noncryptographic approaches. Moreover, the pros and cons of the presented approaches are reported and compared in light of different viewpoints. Furthermore, some new directions are highlighted based on the insightful comparison of the existing work.

Keywords-Digital rights management; privacy-preserving; Authentication

I. INTRODUCTION

As an emerging tool for protecting digital media, digital rights management (DRM) is able to offer an unprecedented level of control over digital content. Digital rights management is mainly used during four basic processes: protection, distribution, management and control. The general digital rights management model consists of four main parts: content provider, server provider, license provider and user.

The main contributions of this paper are twofold: 1) Not only presenting a comprehensive survey of the credible efforts that intend to address security and privacy issues in DRM system, but also investigating how these approaches meet the security requirements. 2) Highlighting some new directions in the DRM system approaches with regard to improving efficiency and reduction of trust on third party, thus paving the way for future efforts.

A. Security Issues in DRM System

According to previous researchers, the security requirements of DRM system are summarized as follows:

Confidentiality: The media content should be encrypted.

Anonymity: The relationship between the end user and corresponding service providers must be concealed so that no service provider able to retrieve user's personal information, such as user identity, IP address, etc.

Integrity: It must be ensured that any digital content used in the context of content distribution has not been changed in the path from content providers to the end user.

Authenticity: It is a requirement for ensuring and assessing the truth of any declaration sourced by a valid entity (content providers, end user and the digital contents).

Flexibility: The license server should support flexible license models.

Efficiency: The online DRM scheme should support efficient license models with low computational complexity to support massive users.

Fine-grained Access Control: The user who satisfies the access policy associated with encrypted content can only consume the contents.

Revocation: The access control rights of the malicious user can be easily revoked. Similarly, the revocation has to be controlled in a fair manner.

Unlinkability: The information obtained from different purchases from the content provider should not be sufficiently established linkability by the unauthorized entities.

Accountability: An obligation to be legally responsible in light of the agreed upon expectations. The users or the content providers are careful and knowledgeable in using the content.

The rest of this paper is organized as follows. In Section two, a survey of the literature on DRM systems is presented. Section 3 presents a comparison of the presented approaches and some new research directions. Finally, the conclusion is introduced in Section 4.

II. A SURVEY OF THE LITERATURE

Encryption is an essential technique for content protection which provides data confidentiality and integrity. Mostly the media contents are encrypted with a content key by the content providers before the distribution. Then, the content key is provided only to authorize users. However, it cannot prevent illegal copy of digital content. Ideally, this problem can be solved by establishing a Digital Rights Management (DRM) capability. This survey focuses solely on the existing privacy-preserving DRM schemes.

Various approaches have been suggested in order to preserve and enhance the privacy of the DRM systems. These approaches are mainly classified into cryptographic approaches and noncryptographic approaches as follows:

1) Cryptographic Approaches:

The cryptographic approaches involve Public Key Cryptography (PKC) approaches and cryptographic primitives approaches. The cryptographic primitives include 1) Identity-Based Encryption, 2) Certificateless public key cryptography (CL-PKC), 3) Proxy Re-encryption (PRE), 4) Attribute-based encryption (ABE). In this section, we briefly

978-1-5090-2535-0/16 $31.00 © 2016 IEEE
DOI 10.1109/ICISCE.2016.82

review the approaches founded on the PKC and other cryptographic primitives that are used to preserve the privacy in DRM systems.

A) PKC-Based Approaches:

In 2009 Sachan et al. [1] proposed a multiparty multilevel (MPML) DRM using PKC and a temporary ID technique. Their architecture uses log files based method for violation detection, which provides an efficient and flexible content distribution mechanism. However, their scheme does not offer any security requirements such as: privacy during the license acquisition process and mutual authentication.

In 2010 Zou et al. [2] proposed a cloud based mobile digital right management scheme with SIM card. Their scheme improves flexibility and reduces the security vulnerability with low cost. In addition, it allows only legal users who have license to consume the digital contents. Nevertheless, the authors applied their phosphor only based on the SIM cards. Also, this scheme requires negotiations about symmetric keys in advance. As a result, this scheme is not practical enough and may reveal the user identity during this negotiation.

Young et al. [3], have proposed a scheme for accountable privacy using verifiable secret sharing, zero knowledge proofs and time capsule. However, this scheme requires trusting a user and two revocation authorities. Furthermore, the user has many extra tasks to do with the proposed scheme.

B) Cryptographic Primitives Approaches:

1. Identity-based encryption (IBE) approaches:

Mishra et al. [4] proposed a hierarchical identity based encryption scheme for multiparty multilevel DRM, which is based on commutative encryption to achieve privacy preservation. However, during the revocation phase the license server can reveal the user identity. Thus, this scheme doesn't achieve the user privacy requirement.

Yang et al. [5], has come up with a novel identity-based DRM system which efficiently reduce the delay of authentication processing. However, in this scheme the mobile user can be authenticated by FAAA server locally instead of sending a query message to HAAA server. Moreover, the user anonymity is a critical issue in such environment when mobile users roam around different networks and they do not want to be tracked by others in order to keep their privacy.

2. Certificateless public key cryptography (CL-PKC) approaches:

In 2013, Mishra et al. [6] proposed certificateless authenticated key agreement protocol for DRM system using the elliptic curve bilinear pairings. Since the pairing over elliptic curve is regarded as one of the highly expensive cryptography primitives [7], the use of such pairings makes the scheme [6] less efficient.

In 2016, Hisham et al. [8] introduced anonymous pairing-free CL-AKE protocol for DRM system, which considered as the more efficient and scalable.

3. Proxy re-encryption (PRE) approaches:

Petrlic et al. [9] also proposed a privacy preserving cloud DRM scheme that allows users to stay anonymous and prevents any party from building user profiles. Employing Ateniese et al. scheme's [10], the authors extends the proxy re-encryption scheme to achieve indistinguishability of first-level ciphertext under the condition that the same second-level ciphertext is re-encrypted for the same party more than once. However, the aforementioned scheme re-encrypt the content every time when the user plays the digital content, which increases both the complexity and the computational cost of the system.

Huang et al. [11] proposed general framework of secure and privacy-preserving digital rights management (DRM) scheme. Their scheme uses homomorphic encryption for key management and proxy re-encryption (PRE) for key distribution. The authors' framework allows content providers to outsource encrypted contents to content server and allows users to play contents with the license issued by the license server. The scheme provides some features: 1) a secure content key distribution scheme; 2) preventing malicious employees of license server from issuing the license to illegal user; 3) achieving privacy preserving; 4) higher efficiency compared with a scheme in [9]. In their framework; however, the license server is configured within the cloud controlled by the cloud service provider. Thus, data owner is required to trust on cloud service provider, which is a semi-trusted part in the cloud [12]. Besides, this scheme only provides a general description without giving a concrete construction.

Joshi et al. [13] proposed a solution towards privacy preserving DRM. The authors used a combination of proxy re-encryption, ring signatures and an anonymous recipient scheme in order to provide unlinkability of content executions. This scheme allows the trusted third party to check the license before the content execution phase. Comparing with the scheme in [9], the main advantage of this scheme is the reduced computation and communication overhead. Nevertheless, this scheme performs not well enough since it uses a number of different cryptographic primitives.

4. Attribute-based encryption (ABE) approaches:

The issues of concurrently achieving the fine-grained access and confidentiality of the encrypted digital content are addressed by Muller et al. [14]. The architecture limits the digital content access to a set of individual users who possess certain properties assigned during the encryption process. In their architecture, the set of rules is divided into two parts, static and dynamic. The static rules are enforced by using ABE before accessing the content, whereas the dynamic rules stored in the license needs to be enforced at runtime by the DRM viewer. However, revocation cannot be achieved in this scheme. What's worse, this scheme is not

applicable for large numbers of users, which may be a huge burden for the server.

Huang et al. [15,16], have proposed an access control scheme based on Ciphertext policy attribute-based encryption (CP-ABE), where the ciphertext is encrypted with an access structure, whereas the corresponding user's private key is created with respect to a set of attributes. Only if the set of attributes associated with a user's private key satisfies the access structure associated with a given ciphertext can the user decrypt the ciphertext. In this sense, the CP-ABE scheme is more suitable for access control in DRM, due to its expressiveness in describing access policy. Their scheme provides both attribute and user immediate revocations without the key update and content re-encryption operations.

A solution to address the security issues particular to the trust required in DRM client and dynamic authorization is presented by Jingyi et al. [17]. The presented paper proposed a secure DRM scheme based on Distributed attribute-based encryption (DABE) and improved Muller et al.'s DRM scheme in [15] by adding action control in the license. The action control is related to user's payment. This scheme has some advantages: 1) achieving fine-grained access control; 2) enabling dynamic authorization; 3) reducing the trust required in DRM client; 4) better robustness.

2) Noncryptographic Approaches:

The noncryptographic approaches mainly possess extra infrastructures in order to be able to participate in the DRM system.

Perlman et al. [18], proposed an anonymous cash payment scheme, in order to allow users to buy content anonymously from the content provider and access the content without being tracked this scheme need anonymization infrastructures, which cost expensive computation and bandwidth. The main disadvantage is that user needs to reveal his real identity to content provider upon receiving anonymous cash.

Conrado et al. [19], proposed a privacy-preserving DRM scheme that is based on smart cards. The users anonymously buy the content from the content provider and that prevents the tracking of users whereas the content is accessed. The authors use a temporary pseudonym techniques which are managed by users' smart cards. Their main assumptions are: 1) users contact the provider by means of anonymous channels, 2). the content can only be accessed by compliant devices. The disadvantages of this scheme are: 1). in the buying phase the content provider may be able to build user profiles by learning the association between the smart card's public key and the content ID, 2). compliant devices under an attacker's control may be knows user and content identities, 3). tracking is possible for a limited number of transactions as the user's pseudonyms change periodically.

Win et al. [20], proposed a privacy preserving content distribution mechanism for DRM without needing TTP. A legitimate anonymous user only can requests a token set from the content owner that allows anonymous purchase of content licenses from content providers. The presented scheme use simple primitives of cryptography such as blind decryption and hash chain to construct the system. A trusted platform module (TPM) also is needed to securely store tokens at the user's computing platform. A drawback is that the entire content is re-encrypted for each content execution.

A solution to the problem of privacy invasion in a multiparty digital rights management scheme is addressed by Petrlic et al. [21]. The scheme allows users to buy content licenses from a content provider and execute it at any nearby content distributor. The presented scheme suggests a privacy-preserving multiparty DRM system based on the smart-card, which does not need any trusted third party to check licenses before allowing content executions.

III. COMPARISON OF THE PRIVACY-PRESERVING

From Table 1 and 2, we can observe that majority of the presented schemes fulfill some requirements, such as integrity, confidentiality. Nevertheless, the requirements, such as anonymity, unlinkability, accountability, revocation and fine-grained access control are met by only a few schemes. There an obvious relationship between the anonymity and unlinkability and most of the presented approaches preserve unlinkability through anonymity. Another great significance observation is related to the ABE-based approaches are: 1) unwanted users having attributes similar to the legitimate users may obtain the decryption keys, 2) costly decryption primitive because of bilinear computations, 3) hard to satisfy user accountability, 4) inefficient access structure, and 5) the presence of the authority does not suits cloud environments. Nonetheless, the ABE approaches have been suitable to achieve a desired level of privacy. We also found that the PKC is considered less efficient in terms of computation. The noncryptographic approaches can never be perfectly secure in a public cloud environment because these approaches are somehow vulnerable to information disclosure by attackers. Nevertheless, noncryptographic approaches are just suits private clouds to achieve a desired level of privacy because the infrastructure in such cases is trusted. Despite all the efforts made to reduce the computational and communication costs, there are still limitations in some aspect.

We propose some new directions aiming to improve the efficiency and reducing the trust on third parties. We briefly highlight the new directions as follows:

In order to improve the efficiency and also reduce the trust assumptions made of the trusted third party significantly, Certificateless Public Key Cryptography (CL-PKC) simplifies the complex certificate management in

TABLE I. COMPARISON OF PRIVACY PRESERVING APPROACHES

Scheme	Technique	Strength	Weakness
Ref [1]	PKC, Pseudonym	Flexible content distribution mechanism	The distributor/owner knows the real identity of consumers
Ref [2]	PKC	Low communication overhead	Applied only with sim cards
Ref [4]	HIBE	Full content anonymity	The license server knows the real identity of consumers
Ref [5]	IBE	The malicious user cannot relay the encrypted content to others	Failed to provide authentication scheme with anonymity
Ref [9]	PRE	prevents profiles building under pseudonym	Huge communication overhead
Ref [11]	PRE, Homomorphic encryption	A secure content key distribution scheme	The scheme without a concrete constraction
Ref [13]	PRE,Ring signatures, An anonymous recipient scheme	Provide different license models	Less performance
Ref [15]	CP-ABE,PRE	Efficient attribute and user revocation	Cost decryption at the user side
Ref [16]	CP-ABE, PRE, Full homomorphic encryption	Dynamic usage control	Cost decryption at the user side
Ref [18]	Anonymization infrastructures, digital signature	No reliance on TTP	Expensive computation cost and band-width
Ref [19]	Trusted hardware device, pseudonyms	No reliance on TTP	Impractical in case of huge number of users
Ref [20]	A trusted platform module (TP-M), Blind decryption, hash chain	No reliance on TTP	The content is re-encrypted for each content execution
Ref [21]	A trusted platform module (TP-M), PRE, pseudonym	No reliance on TTP	Expensive computation cost and bandwidth

TABLE II. SECURITY REQUIREMENTS COMPARISON OF LITERATURE

Security requirement properties	**Design philosophy**							
	Cryptographic Approaches				Noncryptographic Approaches			
	[9]	[13]	[15]	[17]	[18]	[19]	[20]	[21]
Integrity	✓	✓	✓	✓	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓	✓	✓	✓	✓
Authenticity	✓	✓	✓	✓	✓	x	✓	✓
Flexibility	X	✓	✓*	✓*	x	x	✓	✓
Efficiency	X	✓*	✓	✓	x	x	x	x
Unlinkability	X	✓	✓	✓	x	x	x	✓
Accountability	X	x	x	x	x	x	✓	✓
Fine-grained Access Control	X	x	✓	✓	x	x	x	x
Revocation	X	x	✓	✓	x	x	✓	✓
Anonymity	✓	✓	✓	✓	x	x	✓	✓
✓	The scheme satisfies the corresponding property							
✓*	The scheme partially fulfills the property							
x	The scheme does not support the property							

the traditional public key cryptography [7]. To tackle the critical issue of high computation on the user side using ABE approach, outsourcing computation is recommended [22].

Likewise, in ABE approaches, the access policy only supports combining with AND gates and fixed size number of boolean variable inputs. The access policy might be expressed by regular languages with arbitrary size input data. Thus, applying a Deterministic Finite Automata (DFA) scheme [23] is suggested.

IV. CONCLUSIONS

Nowadays, the digital right management system in cloud computing environment has successfully replaced the traditional version; this article conducts a survey on the approaches and methodologies that are currently being used to deal with the important issue of privacy, and classifies these approaches into two main parts: cryptographic and noncryptographic approaches. In addition, we have developed taxonomy of the techniques and presented a comparison of the privacy-preserving approaches from the perspective of the fulfillment of the DRM requirements and key management overhead. Finally, based on this survey we proposed some new directions to address important issues in DRM schemes, which include improving efficiency and reduction of trust on third party.

ACKNOWLEDGEMENTS

The author would like to acknowledge National Natural Science Foundation of China under Grant Nos.61003230, 61370026 and 61202445, the Fundamental Research Funds for the Central Universities under Grant No.ZYGX2013J073 and ZYGX2012J067.

REFERENCES

[1] Sachan. A, Emmanuel. S, Das. A, & Kankanhalli. M~S., Privacy preserving multiparty multilevel DRM architecture. In Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE (pp. 1-5). IEEE, 2009.

[2] Zou. P, Wang. C, Liu. Z, Wang. J & Sun. J. G., A cloud based SIM DRM scheme for the mobile internet. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 759-761). ACM, 2010.

[3] Young-Sam. K, Kim. S. H & Jin. S. H., Accountable privacy based on publicly verifiable secret sharing. In Advanced Communication Technology (ICACT), 2010 The 12th International Conference on (Vol. 2, pp. 1583-1586). IEEE, 2010.

[4] Mishra. D & Mukhopadhyay. S, Privacy preserving hierarchical content distribution in multiparty multilevel DRM. In Information and Communication Technologies (WICT), 2012 World Congress on (pp. 525-530). IEEE, 2012.

[5] C. C. Yang, J. C. Hsiao, and H. W. Yang, Identity-Based DRM in Ubiquitous Multimedia System, In Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference, pp. 270-273. IEEE, 2009.

[6] M. Dheerendra and S. Mukhopadhyay, A certificateless authenticated key agreement protocol for digital rights management system, in Quality, Reliability, Security and Robustness in Heterogeneous Networks, pp. 568-577, Springer, 2013.

[7] H. Debiao and C. Jianhua. An efficient certificateless designated verifier signature scheme, The International Arab Journal of Information Technology, vol. 10, no. 4, pp.389-396, 2013.

[8] H. Abdalla, X. Hu, A. Wahaballa, P. Avornyo, and Q. Zhiguang, "Anonymous Pairing-Free and Certificateless Key Exchange Protocol for DRM System", 2016.

[9] Petrlic. R, Proxy re-encryption in a privac-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,pp. 194-211. 2012.

[10] Ateniese. G, Fu. K, Green. M & Hohenberger. S., Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security (TISSEC), 9(1), 1-30, 2006.

[11] Huang. Q. L, YANG. Y. X, FU. J. Y, & NIU. X. X., Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing. The Journal of China Universities of Posts and Telecommunications, 20(6), 88-95, 2013.

[12] K. Fan, X. Yao, X. Fan, Y. Wang, and M. Chen, A new usage control protocol for data protection of cloud environment, EURASIP Journal on Information Security 2016, no. 1, pp. 1-7, 2016.

[13] Joshi. N, Petrlic. R. Towards practical privacy-preserving digital rights management for cloud computing. In: Proceedings of The 10th Annual IEEE Consumer Communications \& Networking Conference (CCNC 2013). 259{264}, 2013.

[14] Muller. S & Katzenbeisser. S., A new DRM architecture with strong enforcement. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 397-403). IEEE, 2010.

[15] Huang. Q, Ma. Z, Fu. J, Niu. X & Yang. Y., Attribute Based DRM Scheme with Efficient Revocation in Cloud Computing. Journal of Computers, 8(11), 2776-2781, 2013.

[16] Qinlong. H., Zhaofeng. M, Yixian. Y, Xinxin. N & Jingyi. F., Attribute based DRM scheme with dynamic usage control in cloud computing. Communications, China, 11(4), 50-63, 2014.

[17] Jingyi. F, Zhaofeng. M, Qinlong. H & Yixian. Y., Secure DRM Scheme Supporting Dynamic Authorization Using Attribute-Based Encryption. International Journal of Security and Its Applications, 8(4), 287-296, 2014.

[18] Perlman. R, Kaufman. C & Perlner. R., Privacy-preserving DRM. In Proceedings of the 9th Symposium on Identity and Trust on the Internet (pp. 69-83). ACM, 2010.

[19] Conrado. C, Petkovic. M & Jonker. W., Privacy-preserving digital rights management. In Secure Data Management (pp. 83-99). Springer Berlin Heidelberg, 2004.

[20] Win. L. L, Thomas. T & Emmanuel. S., Privacy enabled digital rights management without trusted third party assumption. Multimedia, IEEE Transactions on, 14(3), 546-554, 2012.

[21] Petrlic. R & Sekula. S., Unlinkable content playbacks in a multiparty DRM system. In Data and Applications Security and Privacy XXVII (pp. 289-296). Springer Berlin Heidelberg, 2013.

[22] D. Chaum and T. P. Pedersen, Wallet databases with observer-s, In Advances in Cryptology-CRYPTO'92. Springer Berlin Heidelberg, pp. 89-105, 1993.

[23] Waters. B., Functional encryption for regular languages. In Advances in Cryptology-CRYPTO 2012 (pp. 218-235). Springer Berlin Heidelberg, 2012.