International Journal of Computer Engineering and Information Technology

VOL. 9, NO. 4, April 2017, 67–71
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

Digital Rights Management by Using Cloud Computing

Ku Shyamli Ugale[1], Prof. Ankit Mune[2] and Prof. H.R. Deshmukh[3]

[1, 2, 3] Department of Computer Technology, Sant Gadge Baba Amravati University, India

[1]shyamli2211@gmail.com

ABSTRACT

Cloud computing is an emerging technology which provides various services and storage for a large amount of digital data. The sharing and use of digital information is tremendously increasing in the world. Most of the information is stored in cloud as it provides storage as a service for huge data owners to store their data. This copyrighted data can be easily copied and can Distributed. Thus the security of this digital content is very important. For protecting the digital data the concept of Digital Rights Management was introduced. In DRM environment, only legitimate users are allow to access and use the copyrighted content. It is also equally important to preserve the privacy of the users who is accessing this digital content. For preserving the digital right of the data and privacy of the user various schemes have been proposed some of them rely on a Trusted Third Party (TTP) but there is possibility that the TTP become malicious. We are using an enhance scheme which can preserve both privacy of the user and digital rights of the content without relying on a TTP.

Keywords: *Cloud Computing, Trusted Third Party, Digital Rights Management.*

1. INTRODUCTION

The growth of Internet has made it easy for replicating and distributing digital contents without any loss of quality to the contents. This has resulted in widespread illegal copyright violations of digital contents. Hence, digital rights management (DRM) technologies have been developed to protect the intellectual property rights of the entities involved. Although, advances in DRM technologies have controlled the copyright violations of digital contents, it has resulted in the violations of privacy of the entities involved [7], [9] Privacy preserving DRM schemes using trusted third party assumption have been proposed in [8], [10], [20], [24]. In [24] the authors have proposed a mechanism using anonymity ID for providing privacy in DRM. However, to get an anonymity ID the users need to trust an authentication server that can link all anonymity IDs to the user identities. This problem has been addressed in [8] and [20] by separating the responsibilities between certification authorities and content providers .However, to revoke a user from future use, the trusted parties require to collaborate and link the anonymity ID with the real identity of the user. This weakens the privacy protection to the users as the trusted parties can collude against innocent users. 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. However, their scheme requires trusting a user and two revocation authorities. The trusted third party assumption has been avoided in [7], [9], [15], [18], [25].An anonymous prepayment scheme is used in [25] to get an anonymity ID and thus the real identity of the user is not authenticated in this scheme. [15] uses restrictive partial blind signature method for anonymous consumption of digital contents. However, it does not support tracing and revocation of malicious users. The schemes [7], [9] lacks accounting of sold contents. In threshold based approach essuchase-cash [2], [4] and k-times anonymous authentication [3],[16],the privacy of a user breaks down when the user performs the authentication more than a certain threshold number of times. Tangential.. [18] have provided a privacy preserving accountability mechanism for DRM using "zero-knowledge proofs."However, their mechanism requires many rounds of communications and assumes that user has unlimited computational power.

In this paper, we propose a privacy enabled digital rights management mechanism without using the trusted third party assumption. The proposed mechanism supports both accountability and privacy simultaneously. We use simple cryptographic

primitives such as blind decryption and hash chain to construct the proposed system. We also provide a privacy preserving revocation mechanism which preserves a user's anonymity even after that user has been blocked for its misbehavior. The rest of the paper is organized as follows.The preliminaries and notations given .

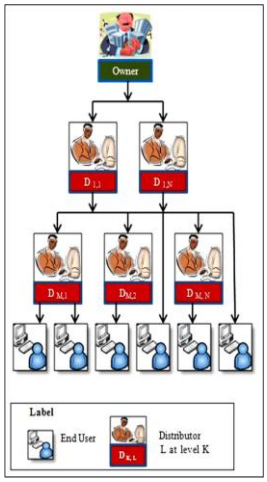

Fig. 1. Content distribution architecture.

NOTATIONS AND PRELIMINARIES

A. Design Goals

A scalable DRM content distribution model involves many entities such as an owner, several distributors and many end users [17], [21]. A typical scalable DRM business model is shown in Fig.1. The content providers (owner and distributors) want a content distribution mechanism that support accounting of the content transactions ,provides security of the content sand makes the users accountable for their actions[13].On the other hand, the end-users and the distributors need the content distribution mechanism to support their privacy and unlink ability concerns [18], [20].

B. Content and License Creation With Access Control

where is a hash function. The Owner encrypts the content with the key .The usage key will be inserted in the usage license and the usage license for the content is created as where is a token used in the content and license purchase, are the requested rights by the user or rights pre defined by the Owner, unique ID of the content .Therefore, only qualified and authentic end-users can get the correct.Similarly, attribute based redistribution key and redistribution license can be created for distribution of contents only by qualified distributors. A content package is composed of two parts: the content header and the encrypted content. The header part stores the content information such as content type, content resolution, required attribute for eligible end users and distributors and other content related information. The Owner stores the content packages in its content server

C. Registration and Acquisition of Anonymous Token

Before communicating with the system for content purchase, each User needs to be registered with the Owner . For a user who requires anonymity, he/she first obtains an Anonymous Token Set Package from the Owner prior to the registration process. Can get an Anonymous Token Set Package only if he/she has first made the payments for the service using an anonymous payment scheme [1], [19]. After making the payment, is provided with a payment receipt with no identity information but with a time stamp signed by the Owner. The presents the receipt to the Owner to get an Anonymous Token Set Package. To use the Anonymous Token Set Package, need the decryption of the key. at a later point (the Owner will not know with which User he/she is interacting) of time requests the decryption of using the following blind decryption protocol [14].

Anonymous Token Set Renewal

When all the tokens in an Anonymous Token Set are expired/used a User will anonymously send a request for renewal with one of its previous Token to the Owner. T he Owner will check it in the Revocation List and its expiry time. If it is not found in the Revocation List and is an expired token, the User will be given an acknowledgement having a timestamp signed by the Owner. User can get another Anonymous Token Set Package and then can proceed to the Owner for the blind decryption of the key as in Section III-C (here no identity authentication is required).

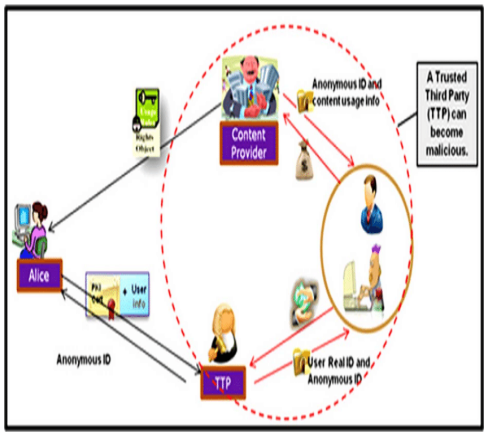

Fig. 2. Malicious third party scenario.

Management of Tokens

At the token generation stage, the Owner store securely in its database the fields .The Content Provider only stores in its secure database where is the ID of the license bought by the User . If at a later stage, the Content Provider detects the violation of the

license by a token, the Content Provider retrieves from its database and send sto the Owner. In the proposed scheme, the Owner and a Content Provider share a token only when a violation of a license is detected. Though they share a token for each violation detected, the Content Provider cannot know the real token ID due to its encryption with the Owner's public key. Only the Owner can decrypt and compute from the real token ID.

2. ANALYSIS AND COMPARISONS

In this section, we carry out the security analysis, complexity analysis and the comparison of the proposed scheme. A. Security Analysis A User needs to perform the authentication with the Owner as a qualified user with its real identity credentials at the registration stage given in the SectionIII –C .The Owner will perform blind decryption for the registered users only. This the scheme satisfies the non-anonymous authentication/registration property. The proposed scheme provides privacy protection to the Users. A User after getting the Anonymous Token Set interacts only with the Anonymous Tokens. Though a User has been authenticated by its real identity in the non anonymous authentication process, the Content Provider or the Owner cannot link the real identity with the anonymous identities of the User in other transactions such as license acquisition, tracking and revocation contents sold by them. To block the Users who are no longer eligible to make content transactions with the Content Providers the revocation of those Users has to be performed. In the proposed scheme, revocation of an anonymous User does not result in the de anonymization of that User as described in Section III-E. A trusted third party (TTP) is an entity that facilitates the interactions between two parties who both trust the third party. In real life a TTP can become untrusted or malicious. In the proposed system the anonymity of the Users are preserved without the need to trust on any third parties. The anonymity of a User is preserved even under collusion of the Owner and the Content Provider. The Content Provider knows the Anonymous Token use in a transaction. However, the Owner cannot identify the User associated with that token as the User had acquired that token through the blind decryption protocol. Our approach prevents a User from sharing his/her Anonymous Tokens with a malicious or illegal user. In order to acquire a license anonymously, a User is required to submit one of the Anonymous Token which was issued to him/her. The Content Provider verifies the authenticity of the token and after successful authentication, the Content Provider stores the token linked to the license in its database. When a violation is detected for the license , the Content Provider can trace back the token linked with the violated license from its database. The blind decryption mechanism suffers from the oracle problem where an adversary can use the decrypt or as an oracle to decrypt encrypted messages for its advantage. In our case, a malicious user may download two different Anonymous Token Set Packages and . In order to use both the Anonymous Token Sets and the malicious user needs to get both the keys and decrypted. We now prove that it is infeasible for a malicious user to get both the keys decrypted. Theorem IV.1: It is computationally infeasible for a malicious user to exploit the "oracle problem" of the blind decryption to get multiple decryption keys. Proof: A Users ends the request for blind decryption along with its PKI certificate and the identity informatin.The owner first verifies whether a blind decryption request has come from this PKI certificate earlier by checking its database. If not it performs the blind decryption and saves the PKI certificate and the identity information of the User in its database. Hence, a User can get only one blind decryption from the Owner. A malicious user is holding two encrypted decryption keys and .In this case, the intention of the malicious user is to find the "best strategy" to get these two keys decrypted using only one blind decryption process. The malicious user needs to input one number derived from and to the blind decryption process. This number should be such that, from the output of the blind decryption, it should be relatively easy to compute the numbers and From, the modular exponentiation step in the RSA decryption algorithm, it follows that this number (the input to the blind decryption process) should be the product . Hence, the malicious user chooses a random blinding factor such that ,computes and sends to the Owner together with its PKI certificate, identity information and the decryption request encrypted with the owner's public key. The Owner decrypts and verifies the PKI certificate and the identity information of the malicious user.

Table 1: Execution Time (In Milliseconds) For Token Generation And Blinding

Operations	Entity	Input Data	Process	Key Size (bit)	Execution Time (ms)	
Token Generation	Owner	Token ID (50 bytes)	SHA-1 Hashing (160 bits)		19.3	
		10 Token IDs (200bytes)	RSA Encryption of 10 Token ID	Key Size	e=65537	e=3
				1024	217	158
				2048	225.16	170
				4096	233	181
				8192	240	203
		Encrypted ID and Timestamp (440 bytes)	RSA Signature Generation	1024	266.19	198.41
				2048	280	219.43
		10 Tokens	3DES Encryption of 10 Tokens	192	159	
			AES Encryption of 10 Tokens	256	90.7	
Blinding	User	Random Integer r (32 bytes)	RSA Encryption of Blinding Factor	2048	$31 \sim 43$	$28 \sim 33$
		x and Encrypted K	Blinding Encrypted key	2048	32	29

Performance Analysis For each Anonymous Token Set Package generation, the major computations need to be performed at the Owner side are: hashing operations, public-key encryptions, digital signature generations, symmetric-key encryptions where is the number of sub tokens in an Anonymous Token Set Package.

The Owner needs to store the Anonymous Token Set Package of all generated token sets.Each one time registration involves 3 round so communication between the Owner and a UserThe Owner and the Content Provider need to store the encrypted token Ids in the Anonymous Token Set for each unexpired and revoked token.

Table 2: Execution Time (In Milliseconds) For License Acquisition Proces

Features	[25]	[15]	[18]	[7]	[8]	Our Scheme
Non-anonymous User authentication	N	Y	N	Y	Y	Y
Content Accountability	Y	N	Y	N	Y	Y
Resistant to Collusion of DRM Servers	Y	Y	Y	Y	N	Y
Anonymous Usage Tracking and Revocation	Y	N	Y	N	N	Y
No Reliance on TTP	Y	Y	Y	Y	N	Y
Prevent Sharing of Anonymity ID	Y	N	Y	N/A	Y	Y
No Extra Computation for User in Transactions	Y	N	N	N	N	Y

C. Experimental Results Generation and the usage of the proposed anonymous token mechanism are independent of the type of the media. We analyzed the computational overheads of the major steps in the proposed mechanism. The details are given below and in the Table. In the token generation process, first a seed value of 50 bytes is randomly selected. Then the seed value for generating the token ID is obtained as follows: the bit of is set as 0 if the bit of is 1 and vice versa, similarly the bit of is set as 0 if the bit of is 1 and vice versa, all the other bits of and are the same. In this way, a unique seed is generated for each token ID.

Comparison with Various Schemes

Most traditional DRM systems use conventional authentication mechanisms based on Public key Certificates. In such DRM systems, Attribute-Based Credentials such as Attribute Certificates are issued after the validation of the Public Key Certificate [6]. The Attribute Certificate will be associated with the Public Key Certificate and the attribute keys. These certificates are required to be present to the party requesting the authentication (eg: Content Provider during license acquisition) which may expose the identity information of the User(e.g.,nameand age) due to linking of the Attribute Certificate with the Public key Certificate. In the proposed system, a User get the attribute keys and a blindly decrypted token after validation of his/her Public key Certificate by the Owner.

3. CONCLUSION

In this paper, we presented a novel privacy enabled digital rights management mechanism without the trusted third party assumption using simple primitives. The proposed scheme satisfies the conflicting requirement of a

ccountability and privacy in digital content distribution. Further, the proposed scheme supports access control without degrading user's privacy as well as allows revocation of even malicious users without violating their privacy. We proved that our scheme is not prone to the "oracle problem" of the blind decryption mechanism. The implementation, analysis and comparison study in Section IV, demonstrate that the proposed scheme is efficient,satisfies the good design properties and out performs the related works.

REFERENCES

[1] R.Ahmadand E.Behza, "Internetcash card,"inU.S.Patent Application 20020143703. : 2002.
[2] M. H. Au, S. S. M. Chow, and W. Susilo, "Short e-cash," Indocrypt, LNCS, vol. 3797, pp. 332–346, 2005.
[3] M. H. Au, W. Susilo, and Y. Mu, "Constant-size Dynamic k-TAA," LNCS, vol. 4116, pp. 111–125, 2006.
[4] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Balancing accountabilityandprivacyusinge-cash,"LNCS,vol.4116,pp.141–155, 2006.
[5] D. Chaum, "Blind signatures for untraceable payments," in Advances inCryptology,ProceedingsofCrypto82. :1983, pp.199–203.
[6] C.N.Chong, R. van Buuren, P. H. Hartel, and G.Kleinhuis, "Security attributes based digital rights management," in Proc. Joint Int. Workshop IDMS/PROMS,2002,vol.LNCS2515,pp.339–352.
[7] D.J.T.ChongandR.H.Deng,"Privacy-enhancedsuperdistributionof layered content with trusted access control," in Proc. ACM Workshop DigitalRightsManagement,Alexandria,VA,Oct.30,2006,pp.37–44.
[8] A.O.DurahimandE. Savas,"A-MAKE:Anefficient, anonymousand accountable authentication framework for WMNs," in Proc. ICIMP, 2010, pp. 54–59. [9] M. Feng and B. Zhu, "A DRM system protecting consumer privacy," in Proc. CCNC, Las Vegas, NV, 2008, pp. 1075–1079.
[9] Y. S. Kim, S. H. Kim, and S. H. Jin, "Accountable privacy based on publicly verifiable secret sharing," in Proc. ICACT, Gangwon-Do, South Korea, 2010, pp. 1583–1586.
[10] L.Lamport,"Password authentication within secure communication," Commun.ACM, vol. 24, no. 11, pp. 770–772, 1981.
[11] S. Michiels, W. Joosen, E. Truyen, and K. Verslype, Digital Rights Management-aSurveyofExistingTechnologiesK.U.Leuven,Dept.of Comput. Sci., Leuven, Belgium, Tech. Rep., 2005.
[12] R. Perlman, C. Kaufman, and R. Perlner, "Privacy-preserving DRM," inProc.9thSymp.IdentityandTrustontheInternet,2010,pp.69–83.
[13] K. Sakurai and Y. Yamane, "Blind decoding, blind undeniable signatures, and their applications to privacy protection," in Proc. 1st Int. Workshop Inf. Hiding, May/Jun. 1996, pp. 257–264.
[14] M.K. Sun, C.S.Laih, H.Y.Yen,andJ.R.Kuo, "Aicketbaseddigital rightsmanagementmodel,"inProc.CCNC,Jan.2009,pp.1–5.
[15] I. Teranishi and K. Sako, "K-times anonymous authentication with a constantprovingcost,"InPublicKeyCryptography,LNCS,vol.3958, pp. 525–542, 2006.
[16] T. Thomas, S. Emmanuel, A. V. Subramanyam, and M. Kankanhalli, "JointwatermarkingschemeformultitipartymultilevelDR Marchitecture," IEEE Trans. Inf. Forens. Sec., vol. 4, no. 4, pp. 758–767, Dec. 2009.
[17] P.P.Tsang,M.H.Au,A.Kapadia,andS.W.Smith,"PEREA: Towards practical TTP-free revocation in anonymous authentication," in Proc. CCS, Alexandria, VA, 2008, pp. 333–344.
[18] Y. Tsiounis, Anonymity & Privacy: The Internet Cash Example [Online]. Available: http://www.internetcash.com/fgo/0,1383,white02,00.Html.
[19] L.Wenjingand R.Kui, "Security, privacy, and accountability in wireless access networks," IEEE Wireless Commun., vol. 16, no. 4, pp. 80–87, 2009. [21] L. L. Win, T. Thomas, S. Emmanuel, and M. S. Kankanhalli, "Secure domain architecture for interoperable content distribution," in Proc. PCM , 2009, vol. LNCS 5879, pp. 1315–1320.
[20] L.L.Win, T.Thomas, and S. Emmanuel, "A privacy preserving content distribution mechanism without trusted third parties," in Proc. IEEE Int.Conf.Multimedia,Barcelona,Spain,2011,pp.1–6.
[21] L. L. Win, T. Thomas, and S. Emmanuel, "Secure interoperable digital content distribution mechanisms in a multi domain architecture," in Multimedia Tools and Applications. New York: Springer-Verlag, 2011.
[22] J. Yao, S. Lee, and S. Nam, "Privacy Preserving DRM Solution With Content Classification and Superdistribution," in Proc. CCNC, Las Vegas, NV, 2009, pp. 1–5.