International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.159-168
http://dx.doi.org/10.14257/ijsia.2014.8.1.15

Towards an Efficient and Secure Online Digital Rights Management Scheme in Cloud Computing

Huang Qinlong[1,2,3], Ma Zhaofeng[1,2,3], Fu Jingyi[1,2,3], Yang Yixian[1,2] and Niu Xinxin[1,2]

[1]*Information Security Center, Beijing University of Posts and Telecommunications, Beijing, China*
[2]*National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing, China*
[3]*Beijing National Security Science and Technology Co., Ltd, Beijing, China*
longsec@bupt.edu.cn, mzf@bupt.edu.cn, fujingyi@bupt.edu.cn, yxyang@bupt.edu.cn, xxniu@bupt.edu.cn

Abstract

Streaming media is widely adopted by thousands of applications in cloud computing, how to effectively protect streaming media contents is a new challenge. In this paper, we propose an efficient online digital rights management (DRM) scheme supporting dynamic license in cloud computing. The content provider encrypts media content and outsources the encrypted content to cloud storage, while the user acquires dynamic license from the license server and consumes the streaming media content from the cloud storage. Further, we present a secure key distribution protocol based on proxy re-encryption, which protects the confidentiality of content encryption key, and reduces the work of key management in the cloud, and also supports domain key to realize user domain management. In addition, we develop a prototype system with Google cloud storage APIs based on the proposed scheme, and the implementation and comparison results show that the proposed scheme satisfies the requirements of online media content protection in cloud computing.

Keywords: *Digital Rights Management (DRM), Online DRM, Proxy Re-Encryption, Cloud Computing*

1. Introduction

With the rapid development of cloud computing and popularization of the standards of multimedia, streaming media is becoming an important network-centric multimedia [1]. Streaming media refers to continuous time-based media which uses streaming transmission technology in the Internet, such as video and audio [2]. Thus consumers can watch online concerts, movies, and television shows in the cloud. The emergence of streaming media accelerates the application of media services, such as online movies and online video on demand. However, illegal copying and dissemination of streaming media damage the legitimate rights of the copyright and content carriers [3]. Digital rights management (DRM) technology is in place to protect digital media from illegal copying and dissemination [4-5].

The industry and academia have proposed many digital rights management solutions. Microsoft and Adobe have released their DRM productions: Microsoft PlayReady and Adobe Flash Access. The OMA and Marlin organization have also developed their practical DRM specifications which are widely applied in real systems [4].

ISSN: 1738-9976 IJSIA

The cloud computing provides large content storages and pay-as-you-go services, which promotes the application of online DRM technology [6]. However, existing online DRM schemes either have poor support on dynamic license models and user domain, or spend much effort on key management. Some of existing online DRM schemes are not suitable for cloud environments, and only support few media format such as Microsoft PlayReady and Adobe Flash Access. These problems and limitations have hindered the popularization of online DRM technology [7].

In this paper, we propose an efficient and secure online digital rights management scheme in cloud computing. In summary, our main contributions are as follows.

1) We propose an efficient online DRM scheme supporting dynamic license in cloud computing. The content provider encrypts media content and outsources the encrypted content to cloud storage, while the user acquires dynamic license from the license server and consumes the streaming media content from the cloud storage. The proposed scheme also allows the user to download and play local protected media content.

2) We present a secure key distribution protocol based on proxy re-encryption. The license server re-encrypts the content encryption key which is encrypted with content provider's public key in advance when the user acquires the license, which protects the confidentiality of content encryption key and reduces the work of key management in the cloud. The protocol also supports domain key to realize user domain management in which a user can share the media content with other domain members.

3) We develop a prototype system with Google cloud storage APIs in Google app engine based on the proposed scheme, and the implementation results show that our scheme satisfies the requirements of online media content protection.

The remainder of this paper is organized as follows: related work is covered in Section 2 and the preliminaries in Section 3. We come up with the framework and detail designs of proposed DRM scheme in cloud computing in Section 4. We present a prototype system with the proposed scheme in Section 5. We analyze the performance in Section 6. Finally we conclude in Section 7.

2. Related Work

Recently, a number of digital rights management schemes have been researched for online scenarios [8-10]. In summary, the DRM technology for online media content is mainly based on digital watermark and digital encryption. Digital watermark is an important technology for copyright protection. The watermark is a signal that is embedded into an original media to protect the media, and can be detected with correlation methods. However, the embedded watermark may be removed or damaged after the malicious attacking.

Compared with digital watermark, DRM scheme based on digital encryption can protect the confidentiality of streaming media. The researchers have proposed many streaming media encryption schemes supporting various format media. Cheng *et al.*, proposed a protection scheme based on online encryption for streaming media [8], which achieves content protection for various-format streaming media by encrypting the streaming data packets. The proposed protection scheme is independent of the streaming server and media format. However, the streaming media stored in the streaming server is plaintext and the proposed scheme which encrypts the streaming media with session key cannot allow the user to download and play local streaming media. Xie *et al.*, proposed a universal streaming media protection system based on

content encryption, and implemented a prototype system of streaming media digital copyright protection [1]. The proposed system has capabilities of transparent supporting local playback and online play of streaming media.

Moreover, flexible usage models and light-weight DRM client have been concerned by academia. Liu *et al.*, proposed rights sharing scheme for online DRM system using digital ticket [9]. The user who receives a valid digital ticket can present the ticket to the right issuer for specified rights. The proposed scheme introduces little overhead to license server, and is secure against multiple-spending and over-issuing attacks. Mampaey *et al.*, presented a network-centric DRM for online scenarios [10]. The key server in the network makes the decision of whether or not deliver the key at playback time, and the end device maintains only the strictly required functions of strong device identification.

The industry also has a variety of commercial online DRM solutions based on digital encryption such as Microsoft PlayReady system and Adobe Flash Access system. In the Adobe Flash Access system, the protected content can be distributed by streaming through Adobe media server, http dynamic streaming, progressive download, or by permitting downloads to a content library for local playback at the consumer's convenience. The system supports a wide range of business models, including video-on-demand and rental. However, usage policies are encrypted into the streaming media for operation purpose, which cannot meet the needs of dynamic license [11-12].

The cloud computing is widely used to provide quality-guaranteed and cost-efficient media streaming services based on large scale content storage and distribution. Xiong *et al.*, proposed a scheme for securely sharing and distributing data via cloud based data storage and content delivery services [13]. The proposed scheme leverages proxy re-encryption algorithm to transfer part of stored ciphertext in the cloud, which can be decrypted by valid user or user groups with secret keys.

Therefore, the requirements for streaming content protection in cloud computing are appeared [13-14]. First, the confidentiality of content stored in cloud storage should be ensured by the content provider. The content provider should encrypt the media content before outsourcing it to the cloud storage. Second, the license server should support flexible license models. The media content may be consumed by different users with different usage rules in the issued license. Meanwhile, the online DRM scheme should support varieties of scenarios including live, on-demand and download and play.

To satisfy the requirements of online media content protection in the cloud, we propose an efficient and secure online digital rights management scheme in cloud computing which reduces the work of key management, and supports flexible license models.

3. Preliminaries

3.1. Bilinear Maps

Let G_1, G_2 be two multiplicative cyclic groups of prime order q, we say a map e is a bilinear map which has the following properties:

1) Computative actions in G_1 and G_2 are efficient.

2) For all $a, b \in Z_q$ of prime order q, and $g, h \in G_1$, $e(g^a, h^b) = e(g, h)^{ab}$.

3) The map e is non-degenerate, which means if g generates G_1 and h generates G_1, then $e(g, h)$ generates G_2.

3.2. Proxy Re-Encryption

Proxy re-encryption allows a proxy to transform a ciphertext computed under A's public key into one that can be opened by B's secret key without any additional decryption. The unidirectional proxy re-encryption scheme is based on the ElGamal scheme operating over two groups G_1, G_2 of prime order q with a bilinear map $e: G_1 \times G_1 \to G_2$. The system parameters in the scheme are $g \in G_1$ and $Z = e(g, g) \in G_2$.

Key Generation (KG): The key generation algorithm generates a public key $PK_A = (Z^{a_1}, g^{a_2})$ and a secret key $SK_A = (a_1, a_2)$ for A, where $a_1, a_2 \in \mathrm{Z}_q$.

Re-Encryption Key Generation (ReKey): A delegates to B by publishing the re-encryption key $RK_{A \to B} = g^{a_1 b_2} \in G_1$, computed by B's public key.

First-Level Encryption (Enc_1): $m \in G_2$ is encrypted under $Z^{a_1} \in PK_A$ by outputting $c = (Z^{a_1 k}, mZ^k)$, where $k \in \mathrm{Z}_q$.

Second-Level Encryption (Enc_2): $m \in G_2$ is encrypted under PK_A by outputting $c = (g^k, mZ^{a_1 k})$, where $k \in \mathrm{Z}_q$. Second-level ciphertext can be re-encrypted to first-level ciphertext.

Re-encryption (ReEnc): Anyone can change a second-level ciphertext for A into a first-level ciphertext for B with $RK_{A \to B} = g^{a_1 b_2}$. From $c = (g^k, mZ^{a_1 k})$, one computes $e(g^k, g^{a_1 b_2}) = Z^{b_2 a_1 k}$ and outputs $c = (Z^{b_2 a_1 k}, mZ^{a_1 k})$.

First-Level Decryption (Dec_1): To decrypt a first-level ciphertext $c = (\alpha, \beta)$ with secret key $a_1 \in SK_A$, one computes for $m = \beta / \alpha^{1/a_1}$.

Second-Level Decryption (Dec_2): To decrypt a second-level ciphertext $c = (\alpha, \beta)$ with secret key $b_2 \in SK_B$, one computes for $m = \beta / \alpha^{1/b_2}$.

4. Proposed Scheme

We propose a secure online DRM scheme in cloud computing. The framework of proposed scheme is shown in Figure 1. The entities involved in the scheme are content provider, cloud storage, streaming server, license server and user or user domain.

Content provider: The content provider encrypts the content with content encryption key, and packages the encrypted data and content encryption key as a whole according to the DRM content format, and outsources the encrypted content to cloud storage. The content provider also generates the re-encryption key for authorized user or user domain.

Cloud storage: The cloud storage stores the encrypted content via cloud, and provides the content to streaming server.

Streaming server: The streaming server receives streaming content access request and transmits the encrypted packet to the user without tying it to any particular transmission mechanism.

License server: The license server authenticates the user and re-encrypts content encryption key from the license acquisition request, and generates the license which includes the content decryption key and usage rules, then distributes the license to the authorized user.

User domain: The user domain is a set of users that shares the same interests. The user can join a user domain and share the domain's secret key in a secure channel. The user also can leave the user domain, and shares the content in the user domain no longer.

Our scheme needn't to store the content encryption key for every media because we encrypt and package the content encryption key in the encrypted content header, which not only ensures the security of content encryption key, but also reduces the work of key management.

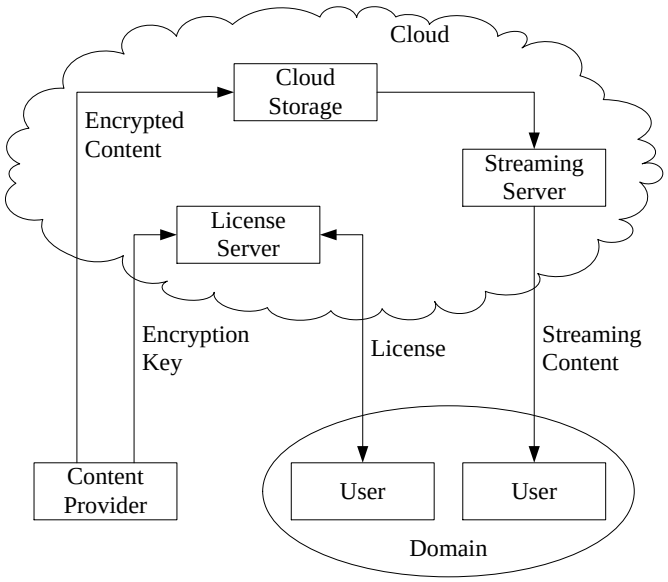

Figure 1. Framework of Proposed Scheme

4.1. Initialization

The scheme first chooses system public parameters, namely $g \in G$ and a bilinear map e. The content provider chooses the public key $PK_{CP} = (Z^{a_1}, g^{a_2})$ and the secret key $SK_{CP} = (a_1, a_2)$, where $a_1, a_2 \in G$. The user chooses the public key $PK_U = (Z^{b_1}, g^{b_2})$ and the secret key $SK_U = (b_1, b_2)$, where $b_1, b_2 \in G$.

The content provider generates the re-encryption key $RK_{CP->U}$ for authorized user and sends the $RK_{CP->U}$ to license server in a secure channel.

$$RK_{CP->U} = ReKey(SK_{CP}, PK_U) = g^{(b_2)a_1} = g^{b_2 a_1}$$

4.2. Content Encryption

In the content encryption phase, the encryption server generates a random key as the *CEK*. Then the content provider encrypts the plain content *PCD* with the *CEK* using symmetric encryption algorithm, and then encrypt the *CEK* with public key PK_{CP} to generate $PEK = (g^k, CEK \times Z^{a_1 k})$, and then packages the encrypted data and *PEK* as the *DCF*.

$$DCF = \{CID \,||\, PEK \,||\, Enc(CEK, PCD)\}$$

4.3. License Acquisition

The user gets the streaming content header from the streaming server and acquires the license from the license server.

Step1: After receiving the *DCF* header, the user extracts the *PEK* from the *DCF* header, and submits the license acquisition request *LCQ* including the *PEK* to license server.

$$LCQ = \{UID \parallel CID \parallel PEK \parallel Sig(SK_U, CID \parallel PEK)\}$$

Step2: When receiving the *LCQ*, the license server checks the signature of *LCQ*, and computes $e(g^k, g^{b_2 a_1}) = Z^{b_2 a_1 k}$, and then re-encrypts *PEK* to output *UEK*.

$$UEK = (Z^{b_2 a_1 k}, CEK \times Z^{a_1 k}) = (Z^{b_2 k}, CEK \times Z^k)$$

Step3: Then the license server generates the license *LIC* which includes content identity *CID*, *UEK*, usage rules *UR*, and digital signature.

$$LIC = \{CID \parallel UEK \parallel UR \parallel Sig(SK_S, CID \parallel UEK \parallel UR)\}$$

The license is designed based on the ODRL specification in this scheme, and supports fine-grained usage control. The license server then distributes the license to the user.

4.4. Content Consumption

After the license server issues the license, the user checks the digital signature of the license with the license server's public key. If the license is valid, the user decrypts the *CEK* from block in the license with private key.

$$CEK = CEK \times Z^k / Z^{(b_2 k)/b_2} = CEK \times Z^k / Z^k$$

Then the user decrypts the content using *CEK* with symmetric encryption algorithm, and consumes the streaming content according to the usage rules in the license.

$$PCD = Dec(CEK, Enc(CEK, PCD))$$

4.5. Domain Management

In the user domain, the user can share the streaming content with other domain members without payment.

1) In the domain generation process, the domain chooses the public key $PK_D = (Z^{d_1}, g^{d_2})$ and the secret key $SK_D = (d_1, d_2)$, where $d_1, d_2 \in G$. The content provider generates re-encryption key $RK_{CP->D}$ for each user domain.

$$RK_{CP->D} = ReKey(SK_{CP}, PK_D) = g^{(d_2)a_1} = g^{d_2 a_1}$$

2) In the domain join process, a user can join one or more user domains and share the domain's secret key SK_D in a secure channel.

3) In the content license acquisition process, when a user in the domain purchases the streaming content and acquires the license from license server, the license server re-encrypts the encrypted *CEK* with the re-encryption key $RK_{CP->D}$.

$$DEK = (Z^{d_2 a_1 k}, CEK \times Z^{a_1 k}) = (Z^{d_2 k}, CEK \times Z^k)$$

4) In the content consumption process, the license server generates the license which includes *DEK*. The members in the user domain can get the license from license server and decrypt the *CEK* with SK_D when they consume the content online in their own client.

5. Prototype System

We performed a prototype system to show the applicability of the proposed scheme. The cloud storage is implemented with Google cloud storage APIs in Google app engine. The content is encrypted with AES 128-bit encryption algorithm and outsourced to Google cloud storage.

As shown in Figure 2, the license server first authenticates the user when the user starts to consume the streaming content, and then distributes the issued license to the user. The user can decrypt the streaming content packets with the corresponding license.

6. Performance Analysis

6.1. Efficient

In our scheme, the license and the encrypted content are delivered separately, and the license server generates the license according to the different license acquisition request. Thus our scheme can support flexible license models, like execute at most n-times models.

Moreover, the proposed online DRM scheme can be used in varieties of scenarios, such as live, on-demand and download and play, and supports flexible transport mechanism, such as streaming, download and progressive download.

(a) User authentication

(b) Online Consumption

Figure 2. Prototype System of Proposed Scheme

6.2. Security

Proof 1: Only authorized user can decrypt the protected content in the cloud storage.

The content provider encrypts the content before outsourcing it to the cloud storage. The content provider encrypts the *CEK* with public key, and stores it in the encrypted content header. The user cannot decrypt the content without the corresponding license. The license server issues the license to the authorized user according to the license acquisition request. Therefore, only authorized user can get the legitimate license and decrypt the protected content. The cloud storage also can't leak the content.

Proof 2: Our scheme is resistant against collusion between license server and malicious user.

In the license acquisition phase, the license server utilizes the proxy re-encryption, which has been proven to be secure against the Decisional Bilinear Diffie-Hellman Inversion problem to re-encrypt the *CEK*. The license server and malicious user cannot re-encrypt the *CEK* without the re-encryption key issued by content provider. Based on the proxy re-encryption algorithm, our scheme ensures that outsourced content cannot be compromised and the content provider protects the contents by issuing the re-encryption key to authorized user or user domain.

6.3. Comparison

Our scheme compared with the major online DRM scheme is shown in Table 1. Microsoft PlayReady is an operating system level DRM which supports dynamic license, and supports the user to download and play local encrypted content, but only supports Microsoft media format. While Adobe Flash Access is a streaming content protection scheme which encrypts the rights information in the streaming media and cannot be able to support dynamic license. In Cheng *et al.'s*, scheme [8], the content needs to be encrypted every time when the user consumes streaming content.

Compared with the major online DRM scheme, our scheme supports universal content formats, reduces the work of the key management, and supports dynamic license, local playback and user domain.

Table 1. Comparison with other Online DRM Schemes

DRM scheme	Microsoft PlayReady	Adobe Flash Access	Cheng' scheme [8]	Our scheme
Content format	WMV,WMA,AAC	FLV,F4V	Universal	Universal
Key management	No	No	No	No
Dynamic license	Yes	No	Yes	Yes
License delivery	Hybrid	Separate	Separate	Separate
Local playback	Yes	Yes	No	Yes
User domain	Yes	No	No	Yes

7. Conclusions

With the development of cloud computing and cloud storage, and the popularity of online media, DRM applications will be more widely used. In this paper, we first propose an efficient online DRM scheme supporting dynamic license in cloud computing. The proposed scheme allows the user to consume protected media content in varieties of scenarios including live, on-demand and download and play. Furthermore, we present a secure key distribution protocol based on proxy re-encryption. The license

server re-encrypts the content encryption key which is encrypted with content provider's public key in advance when the user acquires the license, which protects the confidentiality of content encryption key and reduces the work of key management in the cloud. The protocol also supports domain key to realize user domain management in which a user can share the media content with other domain members. In addition, we develop a prototype system with Google cloud storage APIs based on the proposed scheme, and the implementation and comparison results show that our scheme satisfies the requirements of online media content protection.

Acknowledgements

This work has been supported by the National Natural Science Foundation of China under Grant No. 60803157, 90812001, 61272519.

References

[1] X. Jun and L. Chuanzhong, "Research and realization of streaming media digital rights management", Proceedings of the 2011 International Conference on Informatics, Cybernetics, and Computer Engineering, **(2011)**, pp. 457-465.
[2] N. Wee Siong, K. Markus, B. Stéphane and T. Kian Lee, "Towards a privacy-aware stream data management system for cloud applications", International Journal of Web and Grid Services, vol. 7, no. 3, **(2011)**, pp. 246-267.
[3] L. Hsiao Ying and T. Wen Guey, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, **(2012)**, pp. 995-1003.
[4] M. Zhao Feng, F. Ke Feng, C. Ming, Y. Yi Xian and N. Xin Xin, "Trusted digital rights management protocol supporting for time and space constraint", Journal on Communications, vol. 29, no. 10, **(2008)**, pp. 153-164.
[5] C. Hsingbai, L. Weibin, H. Kevin-I.-J. and Y. Changkuo, "A Secure and Cost-Effective Content Protection Scheme for DRM Systems", Journal of Computational Information Systems, vol. 6, no. 5, **(2010)**, pp. 1377-1386.
[6] F. Deng Guo, Z. Min, Z. Yan and X. Zhen, "Study on cloud computing security", Journal of Software, vol. 22, no. 1, **(2011)**, pp. 71-83.
[7] P. Ronald, "Proxy re-encryption in a privacy-preserving cloud computing DRM scheme", Proceedings of the 4th International Symposium on Cyberspace Safety and Security, **(2012)**, pp. 194-211.
[8] C. Jie, C. Jiuxin, L. Jiazhen and L. Bo, "A protection scheme based on online encryption for streaming media", Proceedings of the 1st IEEE International Conference on Ubi-Media Computing and Workshops, **(2008)**, pp. 165-170.
[9] L. Yang, Y. Nenghai and H. Zhuo, "Rights sharing scheme for online DRM system using digital ticket", Proceedings of 2009 International Conference on Management and Service Science, **(2009)**, pp. 1-6.
[10] M. Marcel and V. Álvaro Nunez, "A network-centric DRM for online scenarios", Bell Labs Technical Journal, vol. 17, no. 3, **(2012)**, pp. 129-134.
[11] M. Kevin J., N. Raj and B. Radim, "DRM workflow analysis for over-the-top HTTP segmented delivery", Proceedings of the 2011 IEEE International Conference on Multimedia and Expo, **(2011)**, pp. 1-4.
[12] N. Do Won, L. Jung Soo, K. Jeong Hyun and Y. Ki Song, "Interlock system for DRM interoperability of streaming contents", Proceedings of the 2007 IEEE International Symposium on Consumer Electronics, **(2007)**, pp. 1-4.
[13] X. Huijun, Z. Xinwen, Z. Wei and Y. Danfeng, "CloudSeal: End-to-end content protection in cloud-based storage and delivery services", Proceedings of the 7th International ICST Conference, **(2012)**, pp. 491-500.
[14] J. Nakul and P. Ronald, "Towards practical privacy-preserving digital rights management for cloud computing", Proceedings of IEEE 10th Consumer Communications and Networking Conference, **(2013)**, pp. 265-270.

Authors

Huang Qinlong received BS degree in information security from Yunnan University in 2009. He is currently a PhD candidate at the School of Computer Science, Beijing University of Posts and Telecommunications. His research interest includes Information Security and Cloud Computing Security and Digital Rights Management.

Ma Zhaofeng is an associate professor in the School of Computer Sicence, Beijing University of Posts and Telecommunications. He got the PhD degree from Xi'an Jiaotong University in 2004. His research interest includes Information Security and Network Security and Digital Rights Management.

Fu Jingyi received BS degree in information security from Chongqi University of Posts and Telecommunications in 2012. She is currently a MS candidate at the School of Computer Science, Beijing University of Posts and Telecommunications. Her research interest includes Information Security and Digital Rights Management.

Yang Yixian received the BS degree in Applied Mathematics from Chengdu Institute of Telecommunication Engineering, China, in 1983, the MS degree and PhD degree from Beijing University of Posts and Telecommunications (BUPT), China, in 1986 and 1988, respectively. He is a professor of BUPT from 1992. He is also doctoral supervisor in school of computer science. His research interests are Information and Network Security, Cryptography, Chaos, and Fuzzy Systems.

Niu Xinxin received the BS and MS degree from the Beijing University of Posts and Telecommunications (BUPT) in 1985 and 1988, and the PhD degree from the Department of Electronic Engineering of the Chinese University of Hong Kong. She is a professor and doctoral supervisor in School of Computer Science of BUPT. Her research areas include Information and Network Security, Information Hiding and Digital Watermark, Digital Content and Security.