Attribute Based DRM Scheme with Efficient Revocation in Cloud Computing

Qinlong Huang[1,2,3], Zhaofeng Ma[1,2,3], Jingyi Fu[1,2,3], Xinxin Niu[1,2], Yixian Yang[1,2]
1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China
3. Beijing National Security Science and Technology Co. Ltd, Beijing 100086, China
Email: longsec@bupt.edu.cn

***Abstract*—The existing digital rights management (DRM) schemes in cloud computing introduce a heavy computation overhead on the content provider for key distribution. In this paper, we propose an attribute-based DRM scheme in cloud computing by combining the techniques of ciphertext-policy attribute-based encryption (CP-ABE) and proxy re-encryption (PRE). We first divide the content encryption key into two parts, content master key and assistant key. Then we enforce access policies based on attributes to distribute the content master key securely. Thus the users who satisfy the access policy can recover the content master key, and then obtain assistant key from the key server and decrypt the content. Furthermore, we achieve efficient attribute and user revocation by allowing the attribute authority to delegate the key server to refuse to issue the assistant key for the revoked users. The security and performance analyses indicate that the proposed scheme is secure, efficient, and privacy-preserving.**

***Index Terms*—digital rights management, attribute-based encryption, proxy re-encryption, fine-grained access control, cloud computing**

I. INTRODUCTION

Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry [1]. The storage services over the cloud, e.g., Microsoft's Azure and Amazon's S3, are a fundamental component of cloud computing, which allow the content providers to outsource their contents to a cloud [2]. Content outsourcing in the cloud relieves the users from building and maintaining their proprietary storage resources, which usually is extremely costly. However, since the cloud service provider (CSP) is semi-trusted, the contents stored in the cloud may be disclosed. Thus, the users need to make sure that their contents are kept confidential in the cloud. The natural way to keep sensitive content confidential against a semi-trusted CSP is to store the encrypted content in the cloud.

The digital rights management (DRM) is a technique to provide methods for content provision, content safekeeping, license creation, content distribution, dynamic authorization and content decryption, which is a popular approach to protect contents [3]. Nowadays numbers of DRM schemes in cloud computing have been proposed based on the techniques of proxy re-encryption (PRE) and attribute-based encryption (ABE).

Not only content confidentiality but also fine-grained access control must be guaranteed in cloud computing environments. To realize fine-grained access control, the traditional DRM schemes either cause high key management overhead, or require encrypting multiple copies of the content with different users' keys [4]. Since content providers and the CSP are usually not in the same trusted domain in cloud computing, fine-grained access control schemes based on attribute-based encryption have been proposed recently [5]. The ABE allows encrypting content by specifying access policy over attributes, so that only users with a set of attributes satisfying the access policy can decrypt the content [6].

However, the major challenges of applying the ABE in DRM are the attribute revocation and user revocation, since each attribute is possessed by multiple users [7]. The traditional revocation schemes usually require the content provider to update the content encryption key, and re-encrypt the content with a new content encryption key, and re-distribute the new content encryption key to authorized users. Thus the revocation operation is difficult and complex since the outsourced contents in the cloud are large in quantity.

In this paper, we propose an attribute-based DRM scheme with efficient revocation in cloud computing. In order to help the content providers to provide confidential contents on cloud servers, we adopt the attribute-based encryption to allow the content provider to selectively provide content among a set of users. We also achieve immediate attribute and user revocation based on proxy re-encryption. Specifically, we make the following main contributions:

(1) We propose an attribute-based DRM scheme by combining the techniques of ciphertext-policy attribute-based encryption and proxy re-encryption. We divide the content encryption key into two parts, content master key and assistant key. The content master key is protected by access policy and distributed to the users with the license, while assistant key is encrypted and stored in the key server. The users who satisfy the access policy can recover the content master key, and then obtain assistant key from key server when they acquire to consume the

doi:10.4304/jcp.8.11.2776-2781

contents. In this way, our scheme enforces fine-grained access control.

(2) We present a scalable revocation scheme by delegating the key server in the cloud to perform the attribute and user revocation. The key server in the cloud refuses to issue the assistant key for the revoked attributes and users, which achieves immediate attribute and user revocation efficiently.

(3) We achieve privacy preserving through allowing the users to stay anonymous towards the cloud service provider and key server in the cloud when they acquire the attribute secret keys and license.

The rest of this paper is organized as follows. Section II reviews the related work. Section III reviews some technique preliminaries pertaining to our construction. Section IV presents our construction. In section V, we analyze our proposed scheme in terms of its security and performance. We conclude this paper in Section VI.

II. Related work

In this section, we review the related work on DRM in cloud computing, attribute-based encryption and revocation in ABE.

A. DRM in Cloud Computing

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. Recently, a number of DRM schemes have been proposed in cloud computing [8-10].

Since content confidentiality and privacy preserving are the major security concerns in cloud computing, Petrlic proposed a privacy-preserving cloud DRM scheme based on proxy re-encryption that allows users to stay anonymous and that prevents any party from building user profiles [8]. This scheme extends the PRE 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.

Petrlic et al. proposed another privacy-preserving DRM concept for cloud computing [9]. The proposed scheme employs a secret sharing scheme based on homomorphic encryption and combines it with a re-encryption scheme to achieve privacy protection.

Perlman et al. proposed a privacy-preserving DRM solution that allows users to buy content anonymously from a content provider and access the content without being tracked [10]. However, these DRM schemes have limited support for different license models.

Muller et al. proposed a new DRM architecture which limits access to media to a subset of users that has to fulfill certain properties [11]. This scheme partitions the set of rules into static and dynamic rules. The static rules are enforced by attribute-based encryption before accessing to the content, while dynamic rules stored in the license must be enforced at runtime by the trusted DRM client. However, revocation is not achieved in this scheme.

B. Attribute-Based Encryption

Attribute-based encryption is a kind of fine-grained public key encryption. In traditional public key encryption, the content provider encrypts content under a public key, and the content provider is assured that only the holder of the corresponding private key can decrypt. While in ABE, the content provider can associate access policy with the content, and only those satisfying the access policy can decrypt the ciphertext.

ABE schemes are classified into KP-ABE and CP-ABE, depending how attributes and access policies are associated with ciphertexts and users' decryption keys. In a CP-ABE scheme, the ciphertext is encrypted with a tree access policy, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given ciphertext, the key can be used to decrypt the ciphertext. A number of works adopted CP-ABE to realize fine-grained access control in cloud computing [12-13]. Wang et al. realized hierarchical attribute-based encryption for cloud storage by enhancing CP-ABE with the technique of hierarchical identity-based encryption [12]. The hierarchical attribute-based encryption clearly is able to cope with more complicated application requirements. Their scheme also enjoys the advantage of delegating heavy workload to the cloud. To support compound attributes, Liu et al. proposed hierarchical ABE encryption for cloud computing [13]. Their construction extends the CP-ABE with the support of hierarchical access structures. In their scheme, each data is associated with an attribute-based access structure and an access time, and each user is identified by a set of attributes and a set of eligible time periods which denote the period of validity of the user's access right.

C. Revocation in ABE

It is a challenging problem to revoke attributes and users efficiently and on-demand in ABE. Several attribute revocable ABE schemes have been proposed recently. Yang et al. proposed a new CP-ABE scheme that resolves the issue of revocation including the entire user access privilege and just partial access right of the user [14]. They realized revocation by revoking attribute itself using timed rekeying mechanism, which is implemented by setting expiration time on each attribute. However, these approaches have two main problems. First problem is the security degradation in terms of the backward and forward secrecy. The other is the scalability problem. The attribute authority periodically announces the unrevoked users to update their keys.

Hence, immediate revocation schemes instead of periodical revocation have been proposed [15-17]. Ibraimi et al. introduces a mediator which maintains a revocation list so as to implement immediate attributes revocation [15]. Yu et al. introduced the semi-trusted agent based on proxy re-encryption [16]. The proxy agent re-encrypts the ciphertext by the latest proxy key, and refreshes all the private keys held by the legal users. Attrapadung et al. proposed a hybrid revocation ABE

scheme by applying a binary tree structure [17]. The data owner may make a choice between the direct revocation model and the indirect revocation model. The data owners and the attribute authority can delegate most of laborious tasks to revocation proxy servers with the technique of proxy re-encryption. However, these revocation schemes will cause the key update operation of large numbers of users.

III. PRELIMINARIES

In this section, we will introduce the basic definitions of ciphertext-policy attribute-based encryption and proxy re-encryption, two cryptographic primitives underlying our construction.

A. Ciphertext-policy Attribute-Based Encryption

The ciphertext-policy attribute-based encryption scheme consists of the following four algorithms:

(1) System setup. The system setup algorithm is a randomized algorithm that takes security parameter as input. It outputs the public key *PK* and a master key *MK*.

(2) Key generation. The attribute key generation algorithm takes as input the master key *MK*, a set of attributes A_U. It outputs a set of private attribute keys ASK_U for user, denotes as $ASK_U = ABE.GenKey(PK, MK, A_U)$.

(3) Encryption. The encryption algorithm is a randomized algorithm that takes as input the public parameter *PK*, a message *M*, and an access structure *AS* over the universe of attributes. It outputs a ciphertext *C* such that only a user who possesses a set of attributes that satisfy the access structure will be able to decrypt the message *M*, denoted as $C = ABE.Enc(PK, AS, M)$.

(4) Decryption. The decryption algorithm takes as input the ciphertext *C* which contains an access structure *AS*, a set of private attribute keys ASK_U. The decryption can be done if the user attributes satisfy *AS*, denoted as $M = ABE.Dec(PK, ASK_U, C)$.

B. Proxy re-encryption

The proxy re-encryption scheme is consisted of the following algorithms:

(1) Key generation. The algorithm takes as input a private key SK_A, a public key PK_B, and outputs a re-encryption key $RK_{A->B}$, denoted as $RK_{A->B} = PRE.GenKey(SK_A, PK_B)$.

(2) Encryption. The algorithm takes as input a public key PK_A and a plaintext *M*, and outputs a ciphertext $C = PRE.Enc(PK_A, M)$.

(3) Re-encryption. The algorithm takes as input a re-encryption key $RK_{A->B}$ and a ciphertext *C* under public key PK_A, and outputs a ciphertext *C*' under public key PK_B, denoted as $C' = PRE.ReEnc(RK_{A->B}, C)$.

(4) Decryption. The algorithm takes as input a secret key SK_B and a ciphertext *C*, and outputs a plaintext $M = PRE.Dec(SK_B, C)$.

IV. OVERVIEW OF OUR SCHEME

A. System Model

We consider the DRM scenario of cloud computing as shown in Figure 1. The system model of the proposed scheme system consists of the following entities:

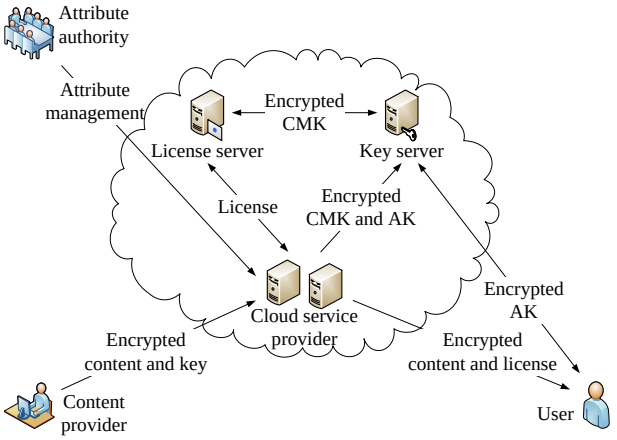

Figure 1. The system model of the proposed scheme

(1) Content provider. This is an entity who wishes to outsource their own contents to cloud storage provided by the CSP, for the purpose of using low-cost and energy-efficient storage resources. The content provider encrypts the contents with the content encryption key before outsourcing. The content encryption key is divided into two parts, content master key and assistant key. The content provider encrypts the content master key with the access structure, and encrypts the assistant key with his public key, and outsources them to the key server through the CSP.

(2) Key server. It is an entity that generates the public and secret keys for content providers and users. It receives the encrypted content master key and assistant key from the users. It also re-encrypts the assistant key for the users when they acquire to consume the contents.

(3) License server. It is an entity which generates and distributes the licenses to the users when receiving the license acquisition from the CSP. The license includes the content master key encrypted with access structure.

(4) Attribute authority. It is a key authority for the attributes set. It generates public and secret parameters for the system. It is in charge of issuing attribute secret keys for users, and delegating the key server to revoke the attributes for users. It also grants differential access rights to individual users based on their attributes.

(5) User. This is an entity who wants to access the outsourced content. If a user possesses a set of attributes satisfying the access structure of the encrypted content master key, and is not revoked, he will be able to acquire the assistant key from the key server and then decrypt and consume the contents.

(6) Cloud service provider. It is an entity that provides content outsourcing and content subscription service. Encrypted contents from the content providers are outsourced to cloud through the CSP, and the CSP is also in charge of content subscription from the users and license distribution to the users.

B. Security Model

Our scheme is designed for the content providers to provide their contents for a set of users in accordance with their respective usage rights. Hence the major security objective is to achieve content confidentiality against unauthorized users.

In our scheme, we consider the cloud service provider to be curious-but-honest. It means that cloud service provider will follow our proposed scheme in general, but try to find out as much secret information of outsourced contents and keys as possible. The cloud service provider may also collude with a small number of malicious users for the purpose of harvesting contents when it is highly beneficial.

As the content providers want to enforce fine-grained access control over their contents in outsourcing, a natural security requirement is that the users cannot obtain contents beyond their authorized usage rights. However, the users would try to access contents either within or outside the scope of their usage rights.

In addition, the communication channel between the content providers/users and cloud service provider are assumed to be secured under existing security protocols such as SSL.

C. Design Goals

The requirements and design goals of DRM scheme in cloud computing are following.

(1) Data confidentiality. Unauthorized users who do not have enough attributes satisfying the access structure should be prevented from accessing the plaintext of the contents. In addition, the CSP is also prevented from accessing the plaintext of stored contents.

(2) High performance. In the cloud-computing environment, the users may access content anytime and anywhere using any device. When a user wants to access content using a thin client with limited performance capabilities, the proposed scheme should be of high performance. Thus the costs introduced by the attribute based scheme should be low enough, so that the user can successfully retrieve content from the cloud, and then decrypt it using the thin client.

(3) Scalable revocation. The traditional revocation scheme usually requires the attribute authority to periodically re-encrypt content, and re-generate new secret keys to unrevoked users. A more scalable approach is to take advantage of the abundant resources in the cloud by delegating the key server to revoke the attributes and the illegal users instantly and efficiently.

(4) Collusion-resistance. If multiple users collude, they may be able to decrypt an encrypted content by combining their attributes even if each of the users cannot decrypt the content alone. It is essential to resist the collusion by dividing the secret, thus the colluders cannot successfully decrypt the contents.

D. Our DRM Scheme Based on ABE

We will provide a system-level description of the proposed scheme as follows. The notations used throughout the paper are presented in Table 1.

TABLE 1.
NOTIONS IN PROPOSED SCHEME

Notion	Description
PK, MK	system public key and mater key
PK_{CP}, SK_{CP}	public key and secret key of content provider
PK_U, SK_U	public key and secret key of user
A_U	attributes of user
ASK_U	attribute secret keys
AS	access structure
RK	re-encryption key
CMK	content master key
AK	assistant key
CEK	content encryption key
LIC	license

(1) System setup

The attribute authority generates the system public key PK, the system master key MK.

(2) Content provider registration

When a content provider registers to the CSP, the key server generates the public key PK_{CP} and secret key SK_{CP} for the content provider, and then sends the PK_{CP}, SK_{CP} and PK to the content provider in a secure channel.

(3) User registration

When a user registers to the CSP, the key server generates the public key PK_U and secret key SK_U for the user. The attribute authority assigns a set of attributes A_U to the user, and then generates a set of user attribute secret keys ASK_U.

$$ASK_U = ABE.GenKey(PK, MK, A_U).$$

The content providers then generate the re-encryption key $RK_{CP->U}$ for user, and send it to the key server.

$$RK_{CP->U} = PRE.GenKey(SK_{CP}, PK_U).$$

The CSP sends the PK_U, SK_U, ASK_U and PK to the user in a secure channel.

(4) Content encryption

Before outsourcing the content to the cloud, the content provider encrypts the content. The sequence diagram of content encryption is shown in Figure 2.

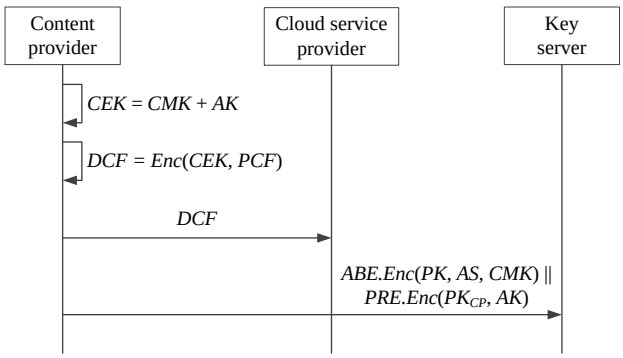

Figure 2. The sequence diagram of content encryption

The content provider first selects a unique *CID*, and generates the content encryption key *CEK* with random content master key *CMK* and random assistant key *AK*.

$$CEK = CMK + AK$$

The content provider then encrypts the blocks of the content *PCF*, and outsources the *DCF* to the CSP.

$$DCF = Enc(CEK, PCF)$$

The content provider defines the attribute-based access structure *AS* for the content, and then encrypts the *CMK* with the *AS* using ABE scheme, and generates the CMK_A.

$$CMK_A = ABE.Enc(PK, AS, CMK)$$

The content provider finally encrypts the *AK* with the public key to generate the AK_{CP}, and sends the CMK_A and AK_{CP} to the key server.

$$AK_{CP} = PRE.Enc(PK_{CP}, AK)$$

(5) License acquisition

The user chooses the interesting content from the CSP, and pays the chosen content. The CSP then sends the license acquisition request including the user's usage rights *UR* to the license server. The license server then acquires the CMK_A from the key server and generates the license which includes the CMK_A, the usage rights *UR*, and the signature *LIS*, then sends the complete license to the user.

$$LIC = \{CMK_A, UR, LIS\}$$

On receiving the license, the user verifies the signature and keeps the license.

(6) Content decryption

When the user wants to access the content, he will first make sure that his attributes satisfy the access structure of the content and he has effective usage rights in the license. If this is the case, the user then acquires the assistant key from the key server. If the user is not revoked, and his attributes related with the access structure of the content are also not revoked, the key server then re-encrypts the *AK* for the user.

$$AK_U = PRE.ReEnc(RK_{CP->U}, AK_{CP})$$

On receiving AK_U, the user recovers the assistant key *AK* with his private key.

$$AK = PRE.Dec(SK_U, AK_U)$$

The user then recovers the *CMK* from the license.

$$CMK = ABE.Dec(PK, ASK_U, CMK_A)$$

The user can finally generate the *CEK* with *CMK* and *AK*, and decrypt the content with the *CEK*.

$$CEK = CMK + AK$$
$$PCF = Dec(CEK, DCF)$$

E. Revocation Scheme

In our revocation scheme, attribute authority delegates the key server in the cloud to implement the attribute revocation and user revocation. The attribute revocation will revoke a user's one or more attributes that he has possessed, which will not affect other users' attributes. While the user revocation will revoke all of a user's attributes.

1) Attribute revocation

Whenever a user's attributes revocation event occurs, the attribute authority will notice the key server in the cloud to check the user's attributes firstly when the user wants to access the encrypted content. If the user's attributes cannot satisfy the access structure of the encrypted content, the key server refuses to re-encrypt the assistant key for the user, and the user cannot access the content.

2) User revocation

Whenever there is a user to be revoked, the attribute authority will inform the key server in the cloud to refuse to re-encrypt the assistant key for the user when the user wants to access the encrypted contents.

Therefore, attribute and user revocation are achieved immediately after the revocation request is made.

V. Performance Analysis

A. Correctness

The correctness of the scheme is straightforward. In the license acquisition phase, the CMK_A is a ciphertext of attribute-based encryption, so if has been granted the attributes, the user should possess the corresponding attribute secret keys for decryption. In the content decryption phase, the key server re-encrypts the AK_{CP} to the AK_U without disclosing the *AK*. Moreover, AK_U is a ciphertext under the user's public key, so only the user can decrypt the *AK* using the private key. With the ability to decrypt the *CMK* and *AK*, the user can certainly decrypt the content.

B. Security

In our proposed scheme, the content provider is able to define and enforce expressive and flexible access structure for each content.

(1) Content confidentiality. The content provider encrypts the contents before outsourcing, thus the cloud service provider cannot disclose the contents, which ensures the content confidentiality. Moreover, the license server which issues the license to the user cannot obtain the content master key, while the key server in the cloud which re-encrypts the assistant key for the user cannot obtain the plain assistant key either. Thus the license server and key server cannot decrypt the content.

(2) Privacy preserving. The user directly communicates with the cloud service provider and key server, and the other parties cannot get any user's personal information. The user anonymously registers to the cloud service provider which distributes the public/private key generated by key server and attribute secret keys generated by attribute authority to the user. In the content decryption phase, the user acquires assistant key from the key server without revealing any personal information. Therefore, the user stays anonymous towards cloud service provider and key server, and the user's privacy is preserved.

C. Performance

We use T_b to represent the attribute-based encryption, T_p to represent the proxy re-encryption, T_a to represent the asymmetric encryption, T_s to represent the symmetric encryption, T_m to represent the modular addition. We analyze computation complexity for content encryption, content decryption. The calculation quantity in content encryption is $T_b + T_a + T_s + T_m$, and the calculation quantity in content decryption is $T_b + T_a + T_s + T_m$.

The comparison of our scheme with related revocation schemes in ABE which support both attribute revocation and user revocation is shown in Table 2. The comparison result indicates that our immediate revocation scheme does not need the key update and content re-encryption operations.

TABLE 2.
COMPARISON OF REVOCATION SCHEME IN ABE

Scheme	Speed	Key update	Content re-encryption
Yang's scheme[14]	Expiry	Yes	Yes
Ibraimi's scheme[15]	Immediate	Yes	No
Yu's scheme[16]	Immediate	Yes	Yes
Our scheme	Immediate	No	No

We also compare our scheme with related DRM schemes, as shown in Table 3. Compared with these DRM schemes, our scheme supports fine-grained access control and privacy preserving. Our scheme also has a relatively low computation cost in content decryption since we achieve attribute and user revocation.

TABLE 3.
COMPARISON OF DRM SCHEMES

Scheme	Fine-grained access control	Attribute/ User revocation	Privacy preserving	Complexity of content decryption
Petrlic [8]	No	No	Yes	$8T_a + T_p$
Muller [11]	Yes	No	N/A	$T_b + T_s$
Our scheme	Yes	Yes	Yes	$T_b + T_a + T_s + T_m$

VI. CONCLUSIONS

Cloud computing is a new revolution in IT, and has the potential to reshape the business model of the IT industry. In this paper, we have proposed an attribute-based DRM scheme by combining the techniques of ciphertext-policy attribute-based encryption and proxy re-encryption. In the proposed scheme, we define and enforce access policy based on attributes to achieve fine-grained access control and privacy preserving. The users who satisfy the access policy can recover the content master key and obtain the assistant key from the key server and decrypt the content. Furthermore, we realize efficient user and attribute revocation by allowing the attribute authority to delegate most of the revocation tasks to key server without disclosing the assistant key. Compared with other DRM schemes in cloud computing, our scheme is highly efficient and provably secure. Our future work will be focused on dynamic usage control in cloud computing.

ACKNOWLEDGMENT

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

REFERENCES

[1] Z. Wan, J. Liu, R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743-754, 2012.

[2] J. Wu, Q. Shen, T. Wang, J. Zhu, J. Zhang, "Recent advances in cloud security," *Journal of Computers*, vol. 6, no. 10, pp. 2156-2163, 2011.

[3] Z. Ma, K. Fan, M. Chen, Y. Yang, X. Niu, "Trusted digital rights management protocol supporting for time and space constraint," *Journal on Communications*, vol. 29, no. 10, pp. 153-164, 2008.

[4] X. Wang, Y. Lin, "An efficient access control scheme for outsourced data," *Journal of Computers*, vol. 7, no. 4, pp. 918-922, 2012.

[5] D. Koo, J. Hur, H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage," *Computers & Electrical Engineering*, vol. 39, no. 1, pp. 34-46, 2013.

[6] M. Luo, C. Zou, J. Xu, "An efficient identity-based broadcast signcryption scheme," *Journal of Software*, vol. 7, no. 2, pp. 366-373, 2012.

[7] J. Hur, D. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, 2011.

[8] R. Petrlic, "Proxy re-encryption in a privacy-preserving cloud computing DRM scheme," *Proceedings of the 4th International Symposium on Cyberspace Safety and Security*, pp. 194-211, 2012.

[9] R. Petrlic, C. Sorge, "Privacy-preserving DRM for cloud computing" *Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops*, pp. 1286-1291, 2012.

[10] R. Perlman, C. Kaufman, R. Perlner, "Privacy-preserving DRM," *Proceedings of the 9th Symposium on Identity and Trust on the Internet*, pp. 69-83, 2010.

[11] S. Muller, S. Katzenbeisser, "A new DRM architecture with strong enforcement," *Proceedings of the 5th International Conference on Availability, Reliability, and Security*, pp. 397-403, 2010.

[12] G. Wang, Q. Liu, J. Wu, M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Computers and Security*, vol. 30, no. 5, pp. 320-331, 2011.

[13] Q. Liu, G. Wang, J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Information Sciences*, 2012.

[14] M. Yang, F. Liu, J. Han, Z. Wang, "An efficient attribute based encryption scheme with revocation for outsourced data sharing control," *Proceedings of 2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control*, pp. 516-520, 2011.

[15] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," *Proceedings of the 10th International Workshop on Information Security Applications*, pp. 309-323, 2009.

[16] S. Yu, C. Wang, K. Ren, W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," *Proceedings of the IEEE INFOCOM 2010*, pp. 1-9, 2010.

[17] N. Attrapadung, H. Imai, "Attribute-Based encryption supporting direct/indirect revocation modes," *Proceedings of the Cryptography and Coding 2009*, pp. 278-300, 2009.