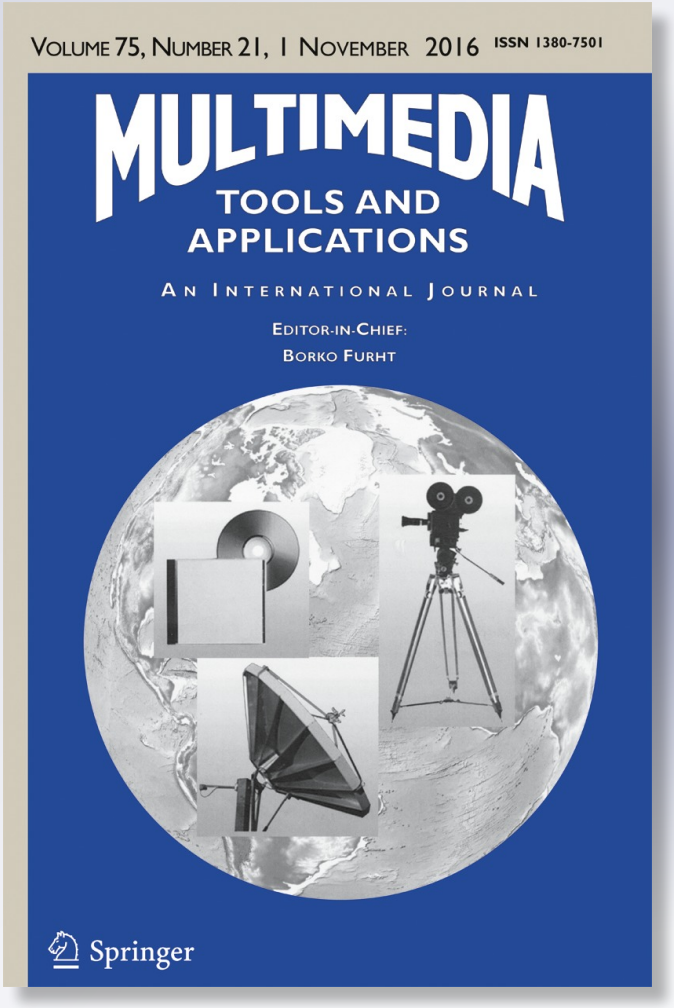
A novel authorization delegation scheme for multimedia social networks by using proxy re-encryption

Weining Feng, Zhiyong Zhang, Jian Wang & Linqian Han

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501
Volume 75
Number 21

Multimed Tools Appl (2016)
75:13995-14014
DOI 10.1007/s11042-015-2929-2



Springer

Multimed Tools Appl (2016) 75:13995–14014
DOI 10.1007/s11042-015-2929-2

A novel authorization delegation scheme for multimedia social networks by using proxy re-encryption

Weining Feng[1] · **Zhiyong Zhang**[1,2] · **Jian Wang**[1] · **Linqian Han**[1]

Received: 5 February 2015 / Revised: 6 August 2015 / Accepted: 31 August 2015 /
Published online: 7 September 2015

Abstract To solve the existing problem of the multimedia social networks platforms, for instance, the copyrighted or private multimedia content can not be safely shared among users, we proposed a novel authorization delegation scheme based on the proxy re-encryption mechanism. This scheme enables one user to delegate digital rights/privileges to another or the group of users, and achieves fine-grained authorization delegation. The ciphertext of content encryption key (CEK) was re-encrypted by the proxy with re-encryption key, which is generated by delegator, and then the ciphertext was sent to the delegatee only who could decrypt the ciphertext. The CCA security of proxy re-encryption was formally proved that this scheme realized the authorization delegation while ensuring the confidentiality of both the sharing content and the delegator's private key. Besides, the privileges can be revoked when the usage control policies have not yet been satisfied. Finally, we demonstrated in detail that the proposed scheme was applied to a multimedia social network prototype called by CyVOD MSN, and it achieved the security share of multimedia content and the functionality of digital rights management, together with better resolving the issue of limited access control list.

Keywords Multimedia social networks · Multimedia security · Authorization · Delegation · Proxy re-encryption · Digital rights management

1 Introduction

Recent years have significantly witnessed that multimedia social networks (MSNs) become more and more popular for the easy, convenient, and fast sharing of content among millions of users who upload images, audios, and videos. However, this convenience and speed in sharing

✉ Zhiyong Zhang
xidianzzy@126.com

[1] Information Engineering College, Henan University of Science and Technology, Luoyang 471023, People's Republic of China

[2] Department of Computer Science, Iowa State University, Ames, IA 50010, USA

content bring several challenges. Access control lists (ACLs) quickly expand because of the large amount of multimedia content in multimedia networks. Large-scale ACLs also decrease data search efficiency. The sharing of copyrighted or private digital content can not ensure the confidentiality of entities' information. The traditional digital rights management (DRM) system focuses mainly on the copyright, and puts less attention to the users' confidentiality and the copyright sharing between more than two users. This authorization delegation scheme can also be applied in the DRM system.

1.1 Delegated authorization of multimedia social networks

Authorization delegation is an act of sublicensing wherein an active entity in the system (for example, a user, an agent that represents a user and its program/process, etc.) delegates its authority to other active entities and allows the authorized entity to perform tasks on behalf of the delegator. This process is executed on the basis of authorization constraints [28] and resource security policies [12] that are set by the delegator. The delegation of users means that the delegator allocates all or part of his/her authority to the delegatee, and the delegatee performs the tasks on behalf of the delegator.

Authorization delegation in multimedia social networks refers to the process in which a user, e.g., Alice, publishes or shares some purchased audio/video contents to the social network after encryption, whereas another user (group), e.g., Bob, requests access to the video that Alice provided authorization. However, users design access control rules and policies [24] for content sharing to protect their privacy [13, 23]. Large-scale and heavy ACLs also decrease an efficiency of searching data. When selling multimedia content, a user needs to delegate authority to the purchasing user under the condition that the former will not reveal his/her account password to the latter.

YouTube has done quite a few of works in order to change the present functions of only providing free digital content and relying on advertisement. For instance, "YouTube Live" is a platform that charges by the play times, and it brings hope to original author. YouTube will mainly develop fee-based business, but the pattern which collects fees just by play times would have passive effect on the development of the business. We could improve the pattern from sharing respect for encouraging users to purchase play right of movies and music. First, the purchased play rights could share with other users. We can define the user in which level could share and how much time he (she) could share. For example, a user *Alice* has the play right for five times, and then she could share with other friends for no more than five times. If a user *Bob* could play the digital content for 20 h, and so he can share the play right within 20 h. Second, there is share problem in personal privacy content. How to share the play right to friends? The simple password would be easily decrypted, and how to send the password to friends is also one of security problems.

1.2 Usage control models and our contributions

The usage control model is combined with and expands the concept of the traditional control models, digital rights management and trust management. The usage control model serves as a framework of comprehensive access control theory and refines the access control discipline [21]. The new features of this model, such as attribute changeability and decision continuity [8], can satisfy the requirement of fine-grained and dynamics in access control under open and distribution environments. Scheme [31] supports dynamic update operations like deletion and insertion of documents in order to increase the flexibility of deletion and insertion. The proposed usage control delegation ($UCON_D$) model [33] enhances that usage decision does

happen at the whole usage procedure features according to the usage control model (UCON). By introducing the proxy re-encryption [30], the proposed scheme which is based on the UCON model realizes the authorization delegation of the audio and video contents in social networks. The delegation scheme which makes the proxy server re-encrypt the ciphertext encrypted by delegator's public key, and the ciphertext could be decrypted by the delegatee's secret key, achieves security delegation.

This scheme does not need the entities to provide any sensitive information and will encrypt the content or information of the delegator and delegatee. It is vital that the proxy just transforms a ciphertext into another ciphertext and is not involved in the generation of a proxy re-encryption key. The proxy server cannot collude with the delegatee to obtain illegal authorization delegation. The access policy in our scheme could be made by the owners themselves and the attribute of user group can be modified dynamically. This scheme focuses on the audio/video content which is involved personal privacy, not only on the sharing data. The rest of this paper is described as follows. Section 2 reviews related research works on authorization delegation and proxy re-encryption briefly. Next, Section 3 describes the authorization delegation scheme and the sending to/back messages between entities. Section 4 gives the proxy re-encryption and formal security proof. And then, an application of the scheme to a prototype called by CyVOD MSN is demonstrated in detail in section 5. Finally, Section 6 summarizes the authorization delegation scheme and comparison and analysis of different schemes.

2 Related works

2.1 Research on authorization delegation

Delegation could be mapping from users into roles, and object into privilege. The paper [25] discusses both role access right administrative privilege delegation and role administrative privilege delegation. The delegation principle mainly includes trust degree and access control policy that is based on the role access control model [14]. In general, the role access control model delegates all rights to another role and can easily cause conflicting authorizations. The scheme [3] introduces an external authorization proxy server to realize the authorization delegation of special content. There is a built-in protected resource manager in the server, and the authorization process is completed by proxy. To solve the authorization delegation problems about the audio and video digital copyright protection on mobile terminals, the scheme [32] achieves arbitrarily sharing between devices by binding digital license to the hardware of the terminal device, and the authorized user could perform the play right. The authorization delegations between users have property of device uncertain,and this scheme is suitable for the scenario of family network or organizations, not the multimedia social networks.

Judging from the fact that the delegation content may involve personal privacy except the owners privacy, [10] improves the general access model which just allow a single controller and allows multiparty (the owner, stakeholder and disseminator) control the data dissemination. The access control policy is complex, and the social network server need store a large number of polices which can lead to ineffective. Since the sensitive data should be encrypted by the data owner before outsourcing, [7] proposed two secure searchable encryption schemes to meet different privacy requirements. The access control provider (ACP) [6] in the protocol uses the access control policy function to protect the data, and the authorization function is realized by the token. The cloud service provider sends this token to the consumer (delegatee).

The access control provider checks the token and certificate of the consumer, and the ACP-signed token is then returned to the consumer. Access control policies are stored in access control provider and access control provider could modify the policy. If the data owner makes access control policies [20], authorization delegation would be more flexible and attract more members. It is flexible that scheme [22] allows users to customize access policies of their data. In the general proxy re-encryption proposal, the proxy is semi-trusted or trusted, but the proxy in scheme [11] is minimally trusted, and it supports fine-grained access control policies and dynamic group membership. Scheme [4] which allows a sender to choose who among the potential delegatees will be able to decrypt his messages.

We aim at proposing a scheme which made policies by users themselves, and guaranteed the delegated content's security. This scheme realizes sharing about the special digital content to one user or several group users without revealing any sensitive information.

2.2 The application of proxy re-encryption

The proxy re–encryption system permits the ciphertext under the public key of the delegator (Alice) to be converted into the ciphertext under the public key of the delegatee (Bob). In this process, the proxy does not obtain any plaintext message. During the authorization, the proxy server obtains the re-encryption privilege and Bob requests the re-encryption result [15]. The unidirectional proxy re-encryption scheme [26] can convert the ciphertext under the public key of Alice into the ciphertext under the public key of Bob but cannot convert the ciphertext under the public key of Bob into the ciphertext under the public key of Alice. The bidirectional proxy re-encryption can convert in reverse. On the basis of the authorized depth, the proxy re-encryption can be classified as single-hop PREs [1] and multi-hop PREs, which difference is single-hop could delegate for one time and multi-hop could delegate for more than one time. The PRE system normally uses a semi-trust proxy which is granted the ability to re-encrypt without being granted the ability to decrypt [2, 17], and the delegator creates the re-encryption key jointly with the delegator. The proposed scheme in this paper is a unidirectional PRE wherein the delegator generates the re-encryption key by himself without the trust of the proxy.

We can classify the data into different categories according to their sensitivity [18]. The PRE system can be used to share access rights in emails, medical records, and university resources [27] and empowers users with delegating capability [16]. When it is not convenient for user to access these resources, the user can delegate his/her access right to a delegatee using PRE. PRE is applied in multimedia social networks for the safe delegation of rights to share data [19] and satisfies the privacy needs of users [5].

3 Descriptions of the proposed scheme

3.1 Structure of the authorization delegation scheme

Table 1 lists all the symbols and their respective descriptions:

3.1.1 Delegator (multimedia content owner)

The owner could purchase some audio and video digital content from YouTube or other social networks, and then he could play digital content several times or within certain period of time.

Table 1 Symbols definitions and descriptions

Symbols	Descriptions
Alice	The purchaser or releaser of the audio/video content acts as the delegator of privilege in this scheme. Alice delegates all or part of the privilege of accessing the audio/video content to other users (groups).
Bob	The receiver (delegatee) of the privilege delegated by the delegator. The receiver can be either a user or a group of users.
MSNS	Multimedia social networks server
Proxy server	Proxy server that can execute PRE operations
m	Audio/video content that is released or purchased by the delegator
CEK	Symmetric key that encrypts the audio/video content
m'	Audio/video content ciphertext after symmetric key has encrypted m
ID_A	Identity information of Alice
ID_B	Identity information of Bob
ID_P	Information of the proxy server
ID_M	Relevant information of the delegated content
AP	Encrypted content authorization policy made by delegator
P	Privilege delegated by the delegator to the delegatee
PK_A,SK_A	Public key of Alice, private key of Bob
PK_B, SK_B	The public key of Bob or the public keys of a group, the private key of Bob or the private keys of a group
CT_A	Ciphertext that is encrypted by the public key of Alice
CT_B	Re-encrypted ciphertext
$\{0,1\}^*$	Cluster of bit strings of any length
$\{0,1\}_n$	Cluster of bit strings with length n
$E_i \wedge E_j$	Occurrence of events E_i and E_j
$a \oplus b$	Connection between the bit strings a and b. These strings have the same length
$a \| b$	The connection between bit strings a and b

How can he share the play right with his friends or family? By setting weak password? Even strong password was been set; there will be security problem about sending the password to delegatee. multimedia social networks will be faced with the same problem when the owner upload some digital content related to personal privacy.

The delegator is responsible for assigning play right to appropriate user, computing ciphertext of CEK and re-encryption key. The delegator sends the ciphertext of CEK and re-encryption key to proxy server after destiny the proxy server.

3.1.2 Delegatee (multimedia shared user/user group)

In general access control model, access control decision is either too loose or too restrictive (e.g., the digital content could be played by any friend or all of them haven't the play right). in order to avoid this, users should be organized in different groups. The name of groups is set by the owner. Usage control policy is either made for group users or several special users.

The delegatee could visit the website and receive the ciphertext which is re-encrypted by proxy server after the delegatee becomes the authorized user. Because the proposed scheme adopts the unidirectional, single hop proxy re-encryption, the delegate cannot share the right any more.

3.1.3 Proxy server

The proxy server should re-encrypt the ciphertext of CEK and send it to the delegatee after received the re-encryption key. Just as we all can see, the proxy server does its duty without learning the underlying plaintext.

3.1.4 Multimedia social networks server

The multimedia social networks server is expected to store the ciphertext of audio/video content, and usage control policy.

Once the delegate uses the authorization right, a temporary attribute will come into being. The temporary is used to record the usage time or duration, and when it is larger than the threshold, the usage right would be revoked.

In multimedia social networks, each user is either a sharer or receiver. The authorization delegation scheme comprises delegator, delegatee, (audio/video sharing) social network server, and proxy server. The delegation structure is illustrated in Fig. 1.

A simple introduction about the basic delegation flow: The delegator Alice and the delegatee Bob are both the members of the same multimedia social networks and they are

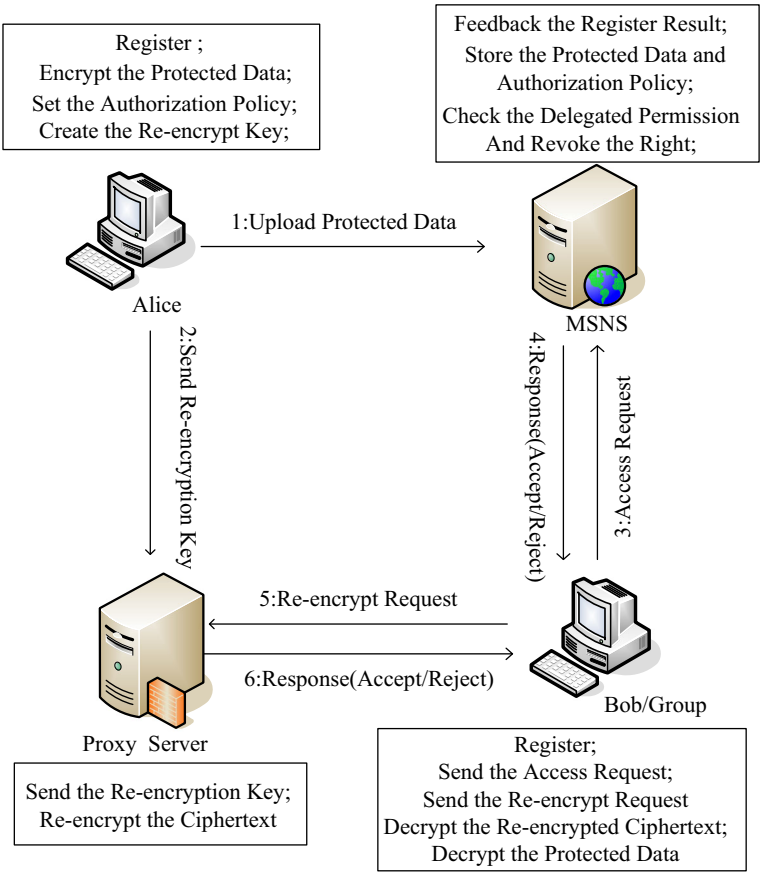


Fig. 1 The architecture of the proposed authorization delegation scheme

friends. Alice purchased or uploaded some audio or video content and would like to share it with Bob. The ciphertext of digital content are stored in multimedia social networks server, and Bob can access this ciphertext. The delegator encrypted the CEK with its public key and computed the re-encryption key. The ciphertext of CEK and re-encryption key would be send to proxy server. Up to now, the secret key of Alice hasn't been sent to anyone.

Bob downloaded the ciphertext of audio or video content, and sent request message to the destiny proxy server. The proxy server re-encrypted the ciphertext of CEK with re-encryption key after receiving the ciphertext of CEK, re-encryption key and request from Bob. According to the information about target delegatee, proxy server sent the re-encryption ciphertext to Bob.

Bob could decrypt the ciphertext of CEK with his secret key, and so that he decrypts the ciphertext of audio or video content. During the period of Bob's usage, the temporary attribute will verify that whether the usage time is larger than zero or play time is larger than threshold.

This delegation scheme is based on the usage control model. The scheme permits updating privilege during the authorization delegation process and continuously controls the privilege after the delegation. The MSNS will revoke the privilege when the privilege time runs out or when the delegatee no longer conforms to the authorization policy. The delegation conditions depend on the group relation between the delegator and delegatee. The multimedia content released by the delegator takes the form of ciphertext that is visible to some or all users. These users can obtain the plaintext through re-encryption or privilege verification.

3.2 The design of the delegation scheme

Alice and Bob registered as members of the same social network. Alice uploads the encrypted content to the MSNs. In addition to storing all the registration information and data access policies of the users, an MSNS can also store the relevant information of various proxy servers, such as proxy ID and proxy that is assigned to specific users. As illustrated in Fig. 2, Alice delegates the privilege of protected audio/video content to Bob.

Grain of encryption: the owner of multimedia contents can divide the contents into groups. The content in the same group is encrypted by the encryption key. The user can set some policies for the user or groups who can be visible to the content.

Dynamic updating of user groups: the control model permits the changing of user attributes and privileges. The delegator needs only to modify the delegatee's group, and the MSNs distribute the corresponding privileges to various groups according to the access policy set by the delegator. Thereafter, the MSNs assign new rights (R) to the delegatees in the changed groups while other information remains unchanged.

Check the usage of privilege: given that the attribute and the delegation policy are both subject to change in the usage model, the MSNs will check the privileges continuously when the delegatee executes the privileges.

The processes of delegation between owner and user group and usage control are as follows:

Alice and her families are both the members of YouTube, and they live in diffident cities. Her families are in the group "family". Alice uploaded her wedding video and wanted to share with her family. She considers that sending it by e-mail or by setting password in the YouTube may be disclosed. This scheme can deal with the problem. After Alice uploaded wedding video, the ciphertext of it can be generated, so the ciphertext was stored in YouTube. YouTube destinies the proxy for Alice so as to issue privilege to delegatee. The content encryption key was encrypted by Alice's public key and stored in YouTube. Then Alice sets up the usage

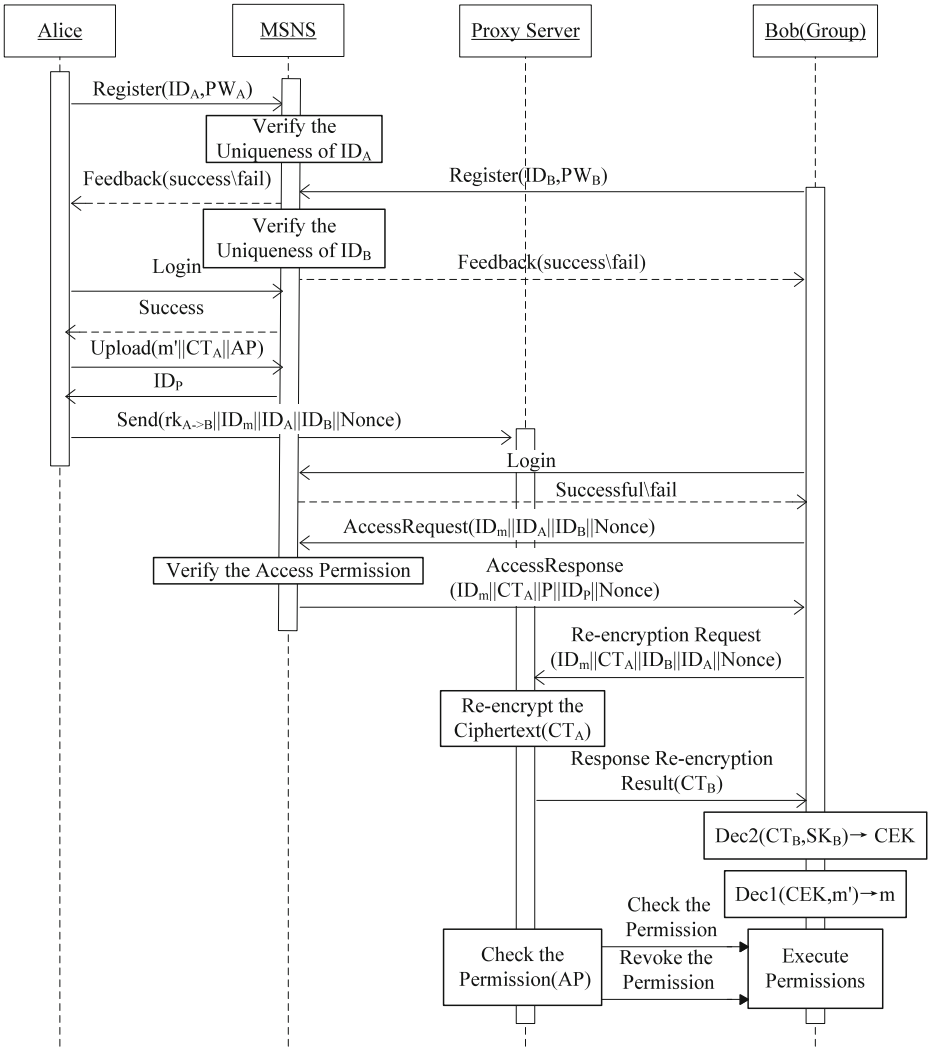


Fig. 2 The sequence diagram of authorization delegation

control policy: the delegate is "family" group and computes the re-encryption key according to her secret key and "family" group's public key. The proxy begins to re-encrypt the ciphertext of content encryption key after received re-encryption key from Alice and re-encryption request from the "family" group. Owing to the fact that proxy re-encryption can convert a ciphertext that is encrypted under Alice's public key into another ciphertext that can be decrypted by family group's secret key, without seeing the underlying plaintext, so the families could decrypt the ciphertext of content encryption key and the YouTube will decrypt the protected data according to the content encryption key which is from family group.

During the usage of delegation right, family group's access right will be checked continuously. If the attribute of a user's group is changed, the corresponding privilege will be revoked. The sensitive information of the delegator's and the delegatee's has never been disclosed until the delegation right is revoked.

The proxy server and YouTube perform the delegation task and usage control without obtaining the plaintext of protected data and content encryption key. Moreover, the confidentiality of Alice's secret key and family group's secret key are insured.

Comparison of the security, confidentiality, flexibility between different schemes is as Table 2:

The major advantages of the scheme are listed as follows:

Device independent: It is well known that users in social network could visit the social networking sites in different devices. If the device is limited to a few special ones, it will make inflexible.

Policy making: The usage control policy could be made by owners themselves, and the policy is executed by social network server. The policy could be made for not only group users, but also a single user.

Key-private: In order to compute re-encryption key, the delegator in bidirectional and general unidirectional proxy re-encryption needs provide secret key to trust or semi-trust proxy. Delegator sends re-encryption key to proxy after computing it. This design is mainly for security reason, and not everything need to be protected. In this way, the scheme realizes the goal of key-private.

Collusion resistance: The proxy cannot compute re-encryption key, so it cann't send re-encrypted ciphertext to the collusive user. Fortunately, the proxy doesn't achieve the plaintext of the content encryption key but the ciphertext to another ciphertext of it.

4 CCA security proof of the proposed delegation scheme

4.1 Bilinear maps and decisional bilinear Diffie–Hellman assumption

4.1.1 Bilinear maps

Let G_1 be the additive cyclic group of a prime order p, which is a large prime number and g is a generator of G_1. G_2 is multiplicative cyclic group of prime order p. Suppose that the discrete logarithm problem in the G_1 and G_2 groups is difficult, and we say that mapping e: $G_1 \times G_1 \rightarrow G_2$ is bilinear mapping if the following conditions hold:

(1) Bilinearity: (g, h) $\in G_1$, and a, b$\in Z_p^*$, then e (g^a, g^b)=e $(g, h)^{ab}$;

Table 2 The comparison results

Schemes	Access control grain	Data confidentiality	Attribute update	Authority revocation	Key private	Access control	Collusion resistance
[22]	Role	ABE	Yes	Yes	No	Access policy	Yes
[11]	Group	ABE	Yes	Yes	No	Access policy	Yes
[4]	One or more delegated users	PRE	Yes	Yes	No	ACL	No
Proposed scheme	User/user group	PRE	Yes	Yes	Yes	Usage control policy	Yes

(2) Non-degeneracy: when $\forall g, h \in G_1$, exists $e(g,h) \neq 1$. The mapping cannot map all $G_1 \times G_1$ elements to the same element in G_2. Given that g is the generator of G_1, e (g, g) is the generator of G_2.

(3) Computable: $\forall g, h \in G_1$ contains a polynomial time algorithm that can compute $e(g,h) \in G_2$.

4.1.2 Decisional bilinear diffie–hellman assumption

Given the tuple $(g, g^a, g^b, g^c) \in {G_1}^4$, then judge if $e(g, g)^z = e(g,g)^{abc}$ exists, $a, b, c \in Z_p$. The advantage of a polynomial time adversary *A* to the DBDH problems of groups (G_1, G_2) is defined as follows:

$$\mathrm{Adv}_{(G1,\,G2),A}^{\mathrm{DBDH}} = \left|\Pr\left[A\left(g,\, g^a,\, g^b,\, g^c,\, e(g,\, g)^{abc}\right) = 1\right] - \Pr\left[A\left(g,\, g^a,\, g^b,\, g^c,\, e(g,\, g)^z\right) = 1\right]\right|$$

We say that the (t, ξ) –DBDH assumption [9, 29] holds if the advantage function $\mathrm{Adv}_{(G1,G2),A}^{\mathrm{DBDH}}$ of adversary *A* is small than ξ, in the arbitrary polynomial time.

4.2 The chosen-ciphertext security of the proxy re-encryption scheme

Game 1: The ciphertext CCA security model for unidirectional proxy re-encryption scheme

The following is an attack game between challenger *B* and adversary *A*. Assume that adversary *A* is given a decryption oracle to define the chosen ciphertext security of proxy re-encryption.

(1) Phase1 Adversary *A* inquires about the oracle.

The public key generation query O_{pk} (i): Challenger *B* inputs the global parameter, executes algorithm KeyGen (pp) to obtain a pair of public and private keys (pk_i, sk_i), and returns pk_i to adversary *A*.

The private key generation query O_{sk} (pk_j): Challenger *B* inputs the global parameter, adversary *A* inputs the public key pk, and challenger *B* returns the corresponding sk_j to adversary *A*.

The re-encryption key generation query O_{ReKenGen} (pk_i, sk_j): Challenger *B* inputs the global parameter and adversary *A* inputs (pk_i, sk_j). Challenger *B* returns to re-encryption key $rk_{i \to j}$=ReKeyGen (sk_i, pk_j).

Decryption query O_{Dec} (pk_j, C_j): adversary *A* inputs (pk_j, C_j), whereas challenger *B* executes the decryption algorithm Dec (sk_j,C) and returns the result to adversary *A*.

(2) Challenge If adversary *A* decides that the query in Phase1 is over, it chooses two messages (m_0 and m_1) and the public key PK_i of the target user as outputs. Challenger *B* takes the public key as an input and randomly selects bit $b \in \{0, 1\}$, encryption message m_b to obtain and return the challenge ciphertext C_i= Enc2 (PK_i, m_b) to adversary *A*.

(3) Query Phase2 The public key generation query O_{pk} (i): Challenger *B* inputs the global parameter pp, executes algorithm KeyGen (pp) to obtain a pair of public and private keys (pk_i, sk_i), and returns pk_i to adversary *A*.

Private key generation query O_{sk} (i): Challenger *B* inputs the global parameter, while adversary *A* inputs public key pk_j. If $pk_j = pk_i$, challenger

B outputs the error symbol. If (pk_i, pk_j, C_i) is the input of re-encryption oracle O_{ReEnc} (pk_i, pk_j, C_i) and challenger *B* outputs the error symbol, challenger *B* returns the corresponding sk_j to adversary *A*.

Re-encryption key generation query $O_{ReKenGen}$ (pk_i, pk_j): Challenger *B* inputs the global parameter pp, adversary *A* inputs (pk_i, pk_j), and challenger *B* returns the re-encryption key $rk_{i\to j}$=ReKeyGen (sk_i, pk_j).

Decryption query O_{Dec} (pk_j, C_j): adversary *A* inputs (pk_i, pk_j). If (pk_j, C_j)=(pk_i, C_i), challenger *B* outputs the error symbol or executes the decryption algorithm Dec (sk_j, C) before returning the result to adversary *A*.

(4) Guess Adversary *A* outputs b' as the guess of b. If b'=b, then adversary *A* wins the game. The advantage of *A* winning the game is expressed as follows:

$$\mathrm{Adv}(A) = \left|\mathrm{Prob}[b' = b] - 1/2\right|.$$

Within the polynomial time, adversary *A* query the public key generation oracle, the private key generation oracle, the re-encryption key generation oracle and re-encryption oracle, and the decryption oracle. If Adv $(A)\leq\varepsilon$, the CCA security of unidirectional proxy re-encryption is achieved.

4.3 Authorization delegation proxy re-encryption scheme

Given that the encryption and decryption of audio/video takes much time, a symmetric encryption method is applied for the encryption. The encryption key uses this method to achieve a high-level security. The owner delegates the authorization for a multimedia digital content by using the proxy re-encryption method, which means that the encrypted ciphertext of the digital content provider that has been encrypted by the proxy by using the re-encryption key can generate the ciphertext that can be decrypted by the requester. The proxy has not obtained the plain text during the re-encryption to maintain a secure authorization delegation.

The authorization delegation agreement encryption scheme that is realized by the proxy re-encryption method is explained below.

(1) System initialization

Setup (λ): Take security parameter λ as input, pp as the output system public parameter, G_1 as the cyclic additive group of a prime order p, which is a large prime number, g, g_1 as the generator, G_2 as the cyclic multiplicative group of prime order p, and (p, g, G_1, G_2, e) as the bilinear parameters. Allow plain text palace $M\in\{0, 1\}^k$, select random numbers $J\in G_1$, hash function $H_1:\{0, 1\}^*\to Z_p^*$, $H_2:\{0, 1\}^*\to G1^*$, H_3: $G_2\to\{0, 1\}^k$. The global open parameters are {pp, p, g, G_1, G_2, e, J, H_1, H_2, H_3}.

(2) Generation of keys

KeyGen (pp): Select an element $SK_A=x_A$ as the private key of user A from Z_p^* randomly and then compute the public key $PK_A = g^{x_A}$. In the same way, private key of user B $SK_B=x_B$ is generated, the public key of user B $PK_B = g^{x_B}$ is computed, the public key of the user is publicized, and the private keys will be sent to user A and user B secretly.

(3) Encryption

Enc1 (*pp*, *CEK*, *m*)→*m*': The owner of the multimedia content encrypts the content by using a symmetric encryption scheme. The encryption key is *CEK*.

Enc2 (pp, PK_A, CEK)→CT_A: the owner of the multimedia content encrypts the key of the content. Select R∈G_2 and compute S=H_1 (CEK,R). The output ciphertext is CT_A=(A, B, C, D, E, F), where A=g^s, B=H_2 (PK_A,pp), C=e (PK_A,J) $^S R$, D=CEK⊕H_3 (R), E=(CEK‖R) e (g,g)^S and F=H_1 (A,B,C,D,E)^S.

(4) Generation of the re-encryption key

ReKeyGen (pp,SK_A,PK_B): input pp, the private key of user A SK_A. The public key of user B $PK_B = g^{x_B}$ and the re-encryption key $rk_{A\to B}$=(A,U), where $U = g^{x_A - x_B}$.

(5) Re-encryptions

ReEnc (pp, $rk_{A\to B}$,CT_A): Testing whether e (H_2 (pp,PK_A),A) is equal to e (B,g) before re-encrypting the ciphertext CT_A. If they are equal, input the global open parameters pp, re-encrypt key $rk_{A\to B}$, and the encrypted ciphertext CT_A. The re-encryption algorithm ReEnc outputs the re-encryption ciphertext CT_B or the error symbol ⊥ and CT_B=(A,C',D).

(6) Decryption

Dec2 (pp,SK_B, CT_B)→CEK: Testing whether A is equal to g^S and if F is equal to H_1 (A,B,C,D,E)^S before decryption, if they are equal, Bob inputs the public parameter, private key, and re-encrypted ciphertext to decrypt the ciphertext and then restores the content encryption key to plain text.

If CEK=D⊕H_3 (R) and S=H_1 (CEK,R), output content encryption key. If A is not equal to g^S in the encrypted key CEK, output error symbol .

DEC1 (pp,CEK,m')→m: Bob outputs the public parameter, content encryption key, and shared content ciphertext before restoring the shared content to plain text according to the decryption algorithm.

(7) Verification of correctness

CEK and any two pairs of public and private keys (PK_A,SK_A) and (PK_B,SK_B) must satisfy the following conditions:

$$\begin{aligned} &\mathrm{D\ e\ c\ 1}\ (CEK, Enc1(pp, CEK, m)) = m \\ &\mathrm{Dec2}\big(SK_B, \mathrm{ReEnc}\big(\mathrm{ReKeyGen}\big(pp, SK_A, PK_B\big), \mathrm{Enc2}(pp, CEK)\big)\big) = CEK \end{aligned}$$

4.4 CCA security for proxy re-encryption scheme

Theorem 1 suppose that the DBDH assumption of groups (G_1,G_2) holds, the multimedia social networks authorization delegation that is realized by the PRE method satisfies the CCA security.

Proof:

In the random oracle model, suppose that a polynomial time adversary A can attack this scheme and the adversary wins the game with ε advantage. According to the assumption, the advantage of the adversary winning the game could be ignored. Given that the re-encrypted ciphertext cannot be re-encrypted through unidirectional single-hop proxy re-encryption, the adversary can re-encrypt the ciphertext after obtaining the re-encryption key. Therefore, the adversary does not need a query about the re-encryption oracle machine. Given that the adversary that has obtained the content encryption key can decrypt the encrypted digital content, it does not need to provide a decryption query for the encrypted digital content.

There is a DBDH input instance (g, g^a, g^b, g^c, T), where a,b,c∈Z_p^*. Challenger B only tests whether T=e(g, g)^{abc} or not. Challenger B randomly selects μ, ε∈Z_p^* and lets J=$g^{b+\mu}$.

(1) Phase1: Adversary A queries about the following oracles.

Public key oracle O_{pk} (i): Challenger B randomly selects $\rho_i \in Z_p^*$ and sets $x_i=a+\rho_i$, $SK_i=x_i$, selects $c_i \in \{0,1\}$, and supposes that the probability of $c_i=1$ is θ,then the probability of $c_i=0$ is 1-θ. If $c_i=1$, challenger B sets $PK_i = g^{x_i}$. if $c_i=0$, $PK_i = g_1^{x_i}$, returns PK_i to adversary A, and adds the triad (PK_i,x_i, c_i) to list L^{list}. Adversary A then publicizes its public key PK_i.

Private key query O_{sk} (PK_i): Challenger B restores the traid (PK_i, x_i, c_i). If $c_i=1$, then $SK_i=x_i$ is returned to adversary A or challenger B outputs to terminate the game.

Re-encryption key query $O_{ReKenGen}$ (PK_i, PK_j) : Challenger B inputs the global parameter pp and adds the traid (PK_i,x_i,c_i), (PK_j,x_j,c_j), to list L^{list} . Challenger B performs the following operations to generate the re-encryption key:

1) If $c_i=c_j=1$, then $SK_i=x_i$, $PK_i = g^{x_i}$ and $SK_j=x_j$, $PK_j = g^{x_j}$. Challenger B outputs $rk_{i\to j}=(A,U)$, where $U = g^{x_i - x_j}$, and adds (PK_i, PK_j) to list T^{RE}.
2) If $c_i=c_j=0$,challenger B outputs $rk_{i\to j}=(A,U)$ and adds (PK_i, PK_j) to list T^{RE}.
3) If $c_i=0\wedge c_j=1$ or $c_i=1\wedge c_j=0$, challenger B outputs the failure symbol.

Re-encryption query O_{ReEnc} (PK_i, PK_j, CT_i) : Challenger B checks if (PK_i, PK_j, CT_i) is in list T^{RE}. If yes, CT_i is the ciphertext after the re-encryption, and the unidirectional single-hop proxy re-encryption cannot perform the re-encryption for several times. Challenger B outputs the error symbol $\perp$ and then checks if PK_i, PK_j, are in list L^{list}. If not, challenger B outputs error symbol or judges if Equation e (H_2 (pp, PK_i),A)=e (B, g) is supported. If not, the ciphertext is considered ineffective and challenger B returns $\perp$ to adversary A. Challsenger B adds the traids (PK_i, x_i,c_i), (PK_j, x_j, c_j) to L^{list} and conducts the following operations:

If $c_i=0\wedge c_j=1$ or $c_i=1\wedge c_j=0$, challenger B generates the re-encryption key $rk_{i\to j}$, executes the algorithm ReEnc (pp, $rk_{i\to j}$, CT_i), and returns the results to adversary A. (PK_i, PK_j, CT_i) is eventually added to list T^{RE} .

If $c_i=0\wedge c_j=1$ or $c_i=1\wedge c_j=0$ and if challenger B generates $rk_{i\to j}$ to execute re-encryption operation for the adversary and adds (PK_i, PK_j, CT_i) to list T^{RE}, challenger B returns $\perp$ to adversary A.

Encryption query O_{Dec} (PK_j, CT_j): Challenger B checks if PK_j is in list L^{list}. If not, challenger B outputs $\perp$ to terminate the game or performs the following operations:

1) If $c_j=1$, challenger B executes the decryption algorithm Dec2 (pp, SK_j, CT_j) and returns the results to adversary A.
2) If $c_j=0$, challenger B verifies if the equation $A=g^S$, H_1 (A,B,C,D,E)^S=F is supported, and runs the decryption algorithm Dec2 (pp, SK_j, CT_j), then returns the results to adversary A. If the equation is supported, challenger B outputs $\perp$ to terminate the game.

(2) Challenging. If adversary A decides that the query of Phase1 is over, it selects two different messages (CEK',CEK") and the public key of the target user PK_i as outputs. Challenger B selects this public key as the input and selects $\alpha \in \{0,1\}$ randomly. The encrypted message $CT^*=(A^*,B^*,C^*,D^*,E^*,F^*)$ could be sent to challenger A. Challenger B selects $R^* \in G_2^*$ randomly and computes the following:

$A^* = g^C$
$B^* = (g^C)^{\varepsilon}$

$C^* = T \cdot e(g^b, g^c)^{\rho i^*} e(g, g^c)^{\mu \rho i^*} e(g^a, g^c)^{\mu} R^*$
$D^* = CEK_\alpha \oplus H_3(R^*)$
$E^* = (CEK_\alpha || R^*) e(g,g)^C$
$F^* = H_1(A^*, B^*, C^*, D^*, E^*)^C$

When $T = e(g,g)^{abc}$, C^* is considered an effective ciphertext.

(3) Phase2:

Public key query O_{pk} (i): The query of this phase is the same as that of Phase1.

Private key query O_{sk} (i): Challenger B inputs the global parameter and adversary A inputs the public key PK_j. If $PK_j = PK_i$ or (PK_i, PK_j) in T^{RE}, challenger B outputs the error symbol . If (PK_i, PK_j, C_i) is the input of re-encryption oracle O_{ReEnc} (PK_i, PK_j, C_i), challenger B outputs the error symbol or returns the corresponding SK_j to adversary A.

Re-encryption key generation query $O_{ReKenGen}$ (PK_i, PK_j): Challenger B inputs the global parameter pp, while adversary A inputs (PK_i, PK_j). If $PK_i = PK_i^*$ and if PK_i is an input of the private key generation query O_{sk} (i), challenger B outputs the error symbol . The continued operations of challenger B are the same as those in Phase 1.

Re-encryption query O_{ReEnc} (PK_i, PK_j, C): Challenger B inputs the global parameter pp, while adversary A inputs (PK_i, PK_j, C). If $(PK_i, C) = (PK_i^*, C^*)$, challenger B outputs the error symbol or executes the same operations of Phase1.

Decryption query O_{Dec} (PK_j, C_j): Adversary A inputs (PK_j, C_j). If (PK_i^*, PK_j, C^*) in the list T^{RE}, challenger B outputs the error symbol $\perp$or executes the same operations of Phase 1 and returns the results to adversary A.

(4) Guess. Adversary A outputs α' as oracle of α. If $\alpha' = \alpha$, then adversary A wins the game. The advantage of adversary A winning the game is computed as follows:

$$Adv(A) = \left| \Pr\left[\left(g, g^a, g^b, g^c, T = e(g,g)^{abc} \right) \right] - 1/2 \right| \geq \varepsilon$$

Moreover,

$$\left| \Pr\left[B\left(g, g^a, g^b, g^c, T = e(g,g)^{abc} \right) = 1 \right] - \Pr\left[B\left(g, g^a, g^b, g^c, T = e(g,g)^{abc} \right) = 1 \right] \right| \geq \left| \left(1/2 \pm \varepsilon \right) - 1/2 \right|$$

In the polynomial time, A queries the public key generation oracle, the private key generation oracle machine, the re-encryption key generation oracle, the re-encryption oracle, and the decryption oracle. If $Adv(A) \leq \varepsilon$, the unidirectional proxy re-encryption is considered CCA security and Theorem 1 has been proven.

5 The design of multimedia social network

CyVOD MSN is a Multimedia social network prototype that comprehensively includes typical functions, such as publishing digital content online, authorization management, usage control, sublicensing the access right, user recommendation, digital content/users recommendation, and so on.

5.1 Design of the platform

Our multimedia social networks platform is based on B/S architecture, and the platform is shown as the Fig. 3. The website has two major function parts, the foregrounding display

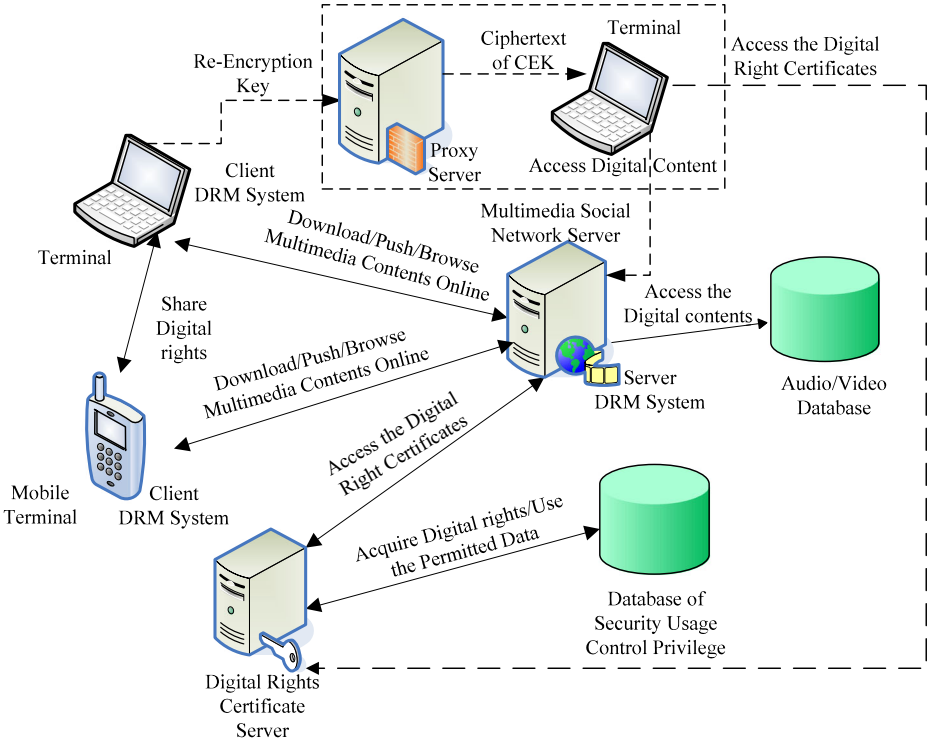


Fig. 3 The architecture of CyVOD multimedia social networks prototype

module and the background management module. The foregrounding mainly to achieve the end users' downloading the encrypted digital content, pushing the multimedia content, previewing and playing the audio/video content online and sharing the purchased or personal content. In addition, there are also making friends, user recommendation, audio/video recommendation and evaluation functions. The background functions mainly include publication of digital content, authorization management, and access control management.

Digital contents of the multimedia social network include visible to all or some special users and encrypted data. The access to encrypted data needs the owner's authorization or the requester to pay for it. To prevent unauthorized access, digital rights certificate server stores digital rights certificate of the encrypted data, and each digital rights certificate has a valid period. The social network server is authorized to issue a digital rights certificate, and so an unauthorized user can not access the digital content for its not getting the digital rights certificate. The access right will be revoked if the access exceeds the time limit.

The module of this scheme is in the dashed frame of Fig. 3, and this scheme realizes authorization delegation with guaranteeing the digital content's confidentiality and security. The audio/video content is encrypted by CEK, and the proxy just re-encrypted the ciphertext of CEK without obtaining the plaintext of CEK and digital content. The proxy sends the ciphertext of CEK to delegatee. The delegatee could decrypt the digital content after decrypted the ciphertext of the CEK. The delegated right which delegator delegated to delegatee will be checked until revoked.

5.2 The flowchart of the general user

The flow chart of general user is presented as Fig. 4. There are two cases of users: registered user could browse the digital content, purchase or share the resources, and check the personal information after passing the identity authentication. Non-registered users only can preview sections of the content, and they could become registered user.

This system distinguishes the registered users according to the trusted degree of the user. The users whose trusted degree is bigger than 0.6 login the web site by the approach of

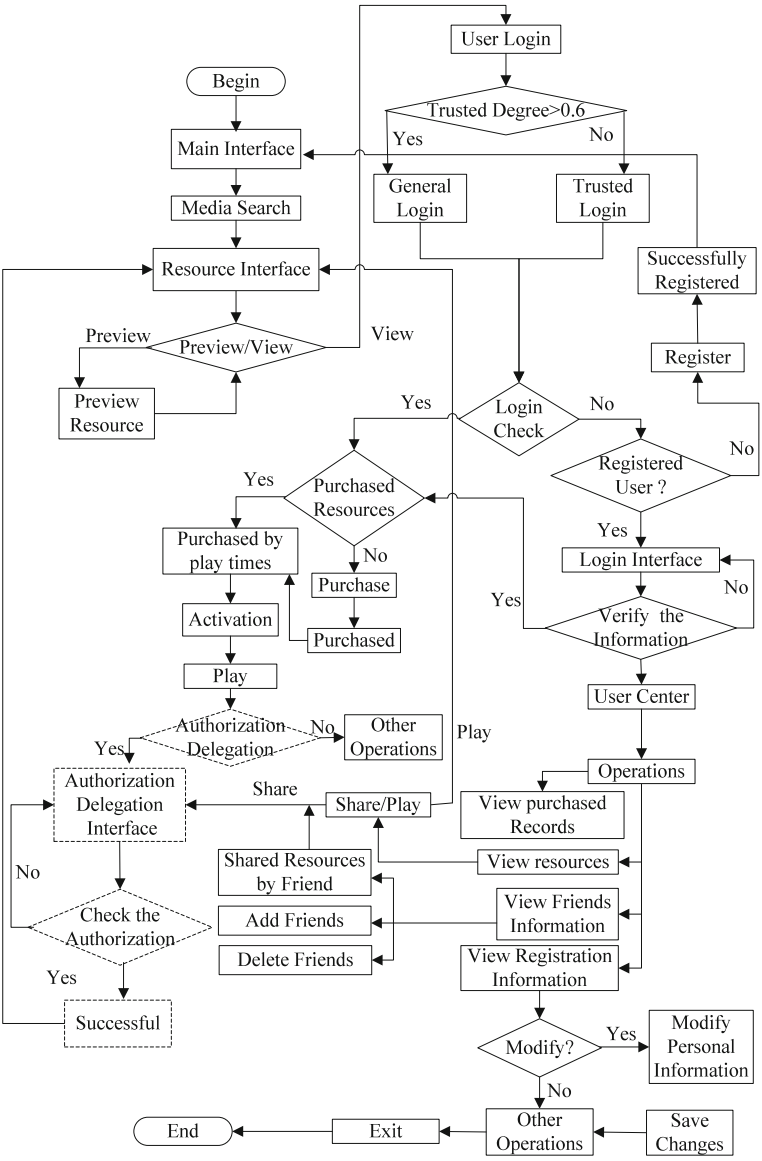


Fig. 4 The usage flowchart for platform users

"general login" and the others login the web site by the approach of "trusted login". Trusted login needs to verify whether the user is trusted while the general login needs not. If the users whose trusted degree is not bigger than 0.6 and the user is trusted user or the users whose trusted degree is bigger than 0.6 could purchase, share or play digital content. The user could buy the audio/video content by play times or time period and delegate it by play times or time period. The system checks the authorization delegation so as to ensure the transmission is controllable.

The function of authorization is presented in dashed frames of Fig. 4. The delegator performs the "authorization delegation" operation and the MSNS checks the delegation according to the relation between them. The authorization delegation records need not be stored in the database with the authorization delegation scheme applied in the system, and so, the problem of large scale ACL can be solved.

6 Conclusions

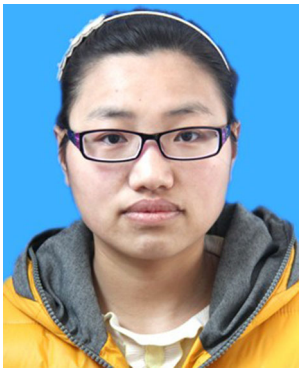
The multimedia social networks authorization delegation scheme could realize security authorization without revealing the private information of entities and the copyrighted content. This scheme that will be applied in the platform CyVOD MSN achieved sharing the digital rights safely and this platform enabled digital rights management getting rid of large access control list. The future work is primarily to study a cross-domain delegation and its dynamic changes of usage control policies, as well as feasible solutions to conflicting authorization delegations.

Acknowledgments The work was sponsored by National Natural Science Foundation of China Grant No.61370220, Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No.15IRTSTHN010, Plan For Scientific Innovation Talent of Henan Province Grant No.134100510006, Program for Henan Province Science and Technology Grant No.142102210425,Key Program for Basic Research of The Education Department of Henan Province Grant No.13A520240 and No.14A520048,Training Foundation for Scientific Innovation Ability of Henan University of Science and Technology Grand No.2013ZCX022, Plan For Innovation Fund for Postgraduates of Henan University of Science & Technology Grant No. CXJJ-ZR12. We give thanks to Dr. Changwei Zhao, Ranran Sun for their technical assistance on CyVOD MSN prototype, and also would like to thank the reviewers and editor for their valuable comments, questions, and suggestions.

References

1. Ateniese G, Benson K, Hohenberger S (2009) Key-private proxy re-encryption. In Proceedings of Cryptographers' Track at the RSA Conference. San Francisco, United States, pp 279–294
2. Blaze M, Bleumer G, Strauss M (1998) Divertible protocols and atomic proxy cryptography. In Proceedings of International Conference on the Theory and Application of Cryptographic Techniques Espoo. Finland, pp 127–144
3. Cui J, Wang X (2009) sns based information authorization delegation mechanism and implementation. In Proceedings of CIS 2009 International Conference on Computational Intelligence and Security. Beijing, China, pp 493–497
4. Devigne J, Guerrini E, Laguillaumie F (2014) Proxy re-encryption scheme supporting a selection of delegatees. In Proceedings of the 7th International Conference on the Theory and Application of Cryptographic Techniques in Africa., Marrakesh, Morocco, pp 13–30
5. Fabian B, Ermakova T, Junghanns P (2015) Collaborative and secure sharing of healthcare data in multi-clouds. Inf Syst 48(3):132–150

6. Fotiou N, Machas A, Polyzos GC (2014) Access control delegation for the cloud. Proceedings of IEEE Conference on Computer Communications Workshops, Toronto, pp 13–18
7. Fu Z, Sun X, Liu Q, Zhou L (2015) Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Trans Commun 98(1):190–200
8. González-Manzano L, González-Tablas AI, de Fuentes JM (2014) SoNeUCONABC: an expressive usage control model for web-based social networks. Comput Secur 43(6):159–187
9. Green M, Ateniese G (2007) Identity-based proxy re-encryption. In Proceedings of 5th International Conference on Applied Cryptography and Network Security. Zhuhai, China, pp 288–306
10. Hu H, Ahn GJ, Jorgensen J (2013) Multiparty access control for online social networks: model and mechanisms. IEEE Trans Knowl Data Eng 25(7):1614–1627
11. Jahid S, Mittal P, Borisov N (2011) EASiER: encryption based access control in social networks with efficient revocation. In Proceedings of the 6th International Symposium on Information, Computer and Communications Security. Hong Kong, China,pp 411–415
12. Kaiiali M, Wankar R, Rao CR (2013) Grid authorization graph. Futur Gener Comput Syst 29(8): 1909–1918
13. Külcü Ö, Henkoğlu T (2014) Privacy in social networks: an analysis of Facebook. Int J Inf Manag 34(6):761–769
14. Li M, Sun X, Wang H (2012) Multi-level delegations with trust management in access control systems. J Intell Inf Syst 39(3):611–626
15. Liang K, Au MH, Liu JK (2014) A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. Futur Gener Comput Syst 52(6):1–13
16. Liang X, Cao Z, Lin H (2009) Attribute based proxy re-encryption with delegating capabilities. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney, NSW, Australia, pp 276–286
17. Liang K, Chu CK, Tan X (2014) Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. Theor Comput Sci 539(6):87–105
18. Liu J, Huang X, Liu JK (2014) Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption. Futur Gener Comput Syst 52(11):1–10
19. Liu Q, Wang G, Wu J (2014) Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Inf Sci 258(2):355–370
20. Martin J, Gunnar D (2012) Usage and impact of model-based user authorization. Inf Resour Manag J 25(3): 98–116
21. Park J, Sandhu R (2004) The UCON ABC usage control model. ACM Trans Inf SystSecur (TISSEC) 7(1): 128–174
22. Qinlong H, Zhaofeng M, Yixian Y (2014) Improving security and efficiency for encrypted data sharing in online social networks. China Commun 11(3):104–117
23. Raji F, Miri A, Jazi MD (2013) CP2: cryptographic privacy protection framework for online social networks. Comput Electr Eng 39(7):2282–2298
24. Ranjbar A, Maheswaran M (2014) Using community structure to control information sharing in online social networks. Comput Commun 41(3):11–21
25. Ruan C, Varadharajan V (2014) Dynamic delegation framework for role based access control in distributed data management systems. Distrib Parallel Database 32(2):245–269
26. Seo JW, Yum DH, Lee PJ (2013) Comments on "unidirectional chosen-ciphertext secure proxy re-encryption. IEEE Trans Inf Theory 59(5):3256–3256
27. Shao J, Cao Z (2012) Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Inf Sci 206(11):83–95
28. Sohr K, Kuhlmann M, Gogolla M (2012) Comprehensive two-level analysis of role-based delegation and revocation policies with UML and OCL. Inf Softw Technol 54(12):1396–1417
29. Son J, Kim D, Hussain R (2014) Conditional proxy re-encryption for secure big data group sharing in cloud environment. In Proceedings of 2014 I.E. Conference on Computer Communications Workshops. Toronto, Canada, pp 541–546
30. Wu TS, Lin HY (2014) Provably secure proxy convertible authenticated encryption scheme based on RSA. Inf Sci 278(9):577–587
31. Xia Z, Wang X, Sun X (2015) A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distrib Syst 99(2):1–13
32. Zhang Z, Wang Z, Niu D (2014) A novel approach to rights sharing-enabling digital rights management for mobile multimedia. Multimedia Tools Appl 6:1–17
33. Zhang Z, Yang L, Pei Q (2007) Research on usage control model with delegation characteristics based on OM-AM methodology. In Proceedings of 2007 IFIP International Conference on Network and Parallel Computing Workshops. Dalian, China, pp 238–243



W. Feng born in 1989 July, is currently a postgraduate majoring in Computer Science, College of Information Engineering, Henan University of Science & Technology. Her research interest focuses on multimedia social networks security and cryptography.

Z. Zhang born in 1975 October, at City of Xinxiang, Henan, China, received his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, respectively. He has been ever Post-Doctoral Research Fellowship at Xi'an Jiaotong University, China. Nowadays, he is a full-time Henan Province Distinguished Professor and Dean with Department of Computer Science, College of Information Engineering, Henan University of Science & Technology. And also, he is a visiting professor of Computer Science Department, Iowa State University. He is ACM Senior Member, IEEE Senior Member, IEEE Systems, Man, Cybernetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Membership for Digital Rights Management Technical Specialist Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee.

Prof. Zhang and research interests include digital rights management and multimedia social networks, trusted computing and access control, as well as security risk management and soft computing. Recent years, he has published over 80 scientific papers and four books on the above research fields, and held 8 authorized patents. Besides, he is Editorial Board Member of Multimedia Tools and Applications and Neural Network World, Associate Editor of Social Network Analysis and Mining, Topic (DRM) Editor-in-Chief of International Journal of Digital Content Technology and Its Applications, as well as Guest Editor of The Computer Journal, EURASIP Journal of Information Security, Journal of Multimedia, etc. And also, he is Chair/Co-Chair and TPC Member for numerous international workshops/sessions on Digital Rights Management and contents security.

J. Wang born in 1978 December, received her Master degree in Huazhong University of Science & Technology and earned her PhD. degree in Tongji University. She is nowadays an associate professor at Electrical Engineering College, Henan University of Science & Technology. Her research interests include Trusted Computing and Trusted Networks Access.

L. Han born in 1989 February, is currently a postgraduate majoring in Computer Science, College of Information Engineering, Henan University of Science & Technology. Her research interest focuses on multimedia social networks security and. Soft Computing.