A NOVEL ATTRIBUTE-BASED ACCESS CONTROL MODEL FOR MULTIMEDIA SOCIAL NETWORKS

Z. Zhang, L. Han, C. Li, J. Wang

Abstract: Multimedia social networks (MSNs) provide great convenience to users, while privacy leaks issues are becoming prominent. The studies on relationship-based access control have been widely used in social networks. However, with the dynamic development of social networks and rapid growth of user information, the access control does not completely meet the current system's need. In this paper, an attribute-based access control model called ABAC–MSN is proposed for MSNs. This model comprehensively considers user attributes, environment attributes and resource attributes, not only including relationships among users. In this model, users can set multimedia usage control policies based on three categories of user-defined attributes. A formal theoretical model is established, which includes constraint rules, data flow rules, policy conflict resolution mechanism, and applied to CyVOD.net, a multimedia social-network-platform prototype systems. The deployment and application denote that this method effectively and flexibly addresses use-case scenarios of multi-attribute-based media access control, and improves the access security of social media platforms and resources.

Key words: *multimedia social networks, attribute-based access control, security, prototype*

Received: April 15, 2016 **DOI:** 10.14311/NNW.2016.26.031
Revised and accepted: October 3, 2016

1. Introduction

With the rapid development of social networks platforms where users can access and share multimedia resources online, multimedia social networks have played a crucial role in daily life. In MSNs platforms, users can quickly and easily share multimedia content with their friends, families and colleagues. These social networks, which have become the most popular networks services in recent years, have attracted a large number of users on a global scale. According to YouTube official statistics report, YouTube has over a billion users, almost a third of all people on the Internet, and every day people watch hundreds of millions of hours of YouTube videos and

Zhiyong Zhang – Corresponding author, Linqian Han, Cheng Li, Jian Wang, Information Engineering College, Henan University of Science and Technology, Kaiyuan Avenue No. 263, Luoyang, China, E-mail: xidianzzy@126.com, hlinqian@126.com, 15991727802@sina.cn, wangjian\protect_migi@sina.com

generate billion of views. While enjoying the convenience of social media, users have also suffered from incidents, such as data theft, information fraud, crimes against privacy and copyright infringement, which are committed by disordered social organizations and hostile participating entities [17, 18]. These incidents are constantly intertwined with security and trust issues [19]. Problems such as privacy leaks and copyright infringement have also become an urgent challenge.

The conventional access controls, including discretionary access control, mandatory access control, role-based access control and trust-based access control [13], are mainly based on labels, such as user identity, group, user role and security label. Role-based access controls or group-based approaches can't truly capture the social relationships among users. These access controls do not adapt to dynamic MSNs. For relationship-based access controls (ReBAC) [7], which is popular used in social networks, the authorization depends on the relationships among users, including their friends, friends of friends, colleagues and families. At present, relationship-based access control is important in protecting user data security and privacy [16]. A ReBAC model uses a different set of properties to define relationships, resulting in a more natural disclosure of personal information. Then, how social aware are current mainstream social media privacy control [11]? However, with the dynamic development of social networks, user information and activities have grown quickly, and the relationship-based authorization decision alone is insufficient to meet user's demands. Therefore, a new access control mechanism is required to meet the needs of different types of users. Here, we primarily consider the following several scenarios:

Scenario 1. Alice is fond of traveling, and she uploads her travel videos and photos to a multimedia platform to share with her friends who have the same interests with her. But, she does not want Eve to view the photos or videos, nor any other of her friends to download or share such photos or videos.

Scenario 2. Dave, a middle school student and a multimedia platform user, spends a large amount of time using multimedia every day. His parents are concerned that this habit might affect his studies and normal life, they hope to limit the time of he spends on it. We assume the users under the age of 18 spend minimal time on multimedia platforms and are typically allowed to browse, share, and tag videos only within a limited period.

Scenario 3. Bob, a VIP user of MSNs platform, can browse, share, and download copyrighted videos. If he shares a video with non-VIP friends, the copyrighted resources may be accessed by non-VIP users.

Scenario 4. Charlie uploads and shares some facetious videos with other users on a multimedia platform. He wants only the people among his classmates group to browse and share the videos, but the others have no rights to access. How can he grant access to Eve, who is both in the group of student and friend?

ReBAC mainly focuses on relationship type and relationship depth, while it is failure to solve the above problems without considering any history messages, some basic user attributes and the current context. Therefore, flexibly implementing the fine-grained access control over multimedia resources requires a suitable access

control mechanism. A new ABAC-MSN model is proposed in this paper, fully considering user attributes, environment attributes and resource attributes, as the main parameters for access permission.

The rest of this paper is organized as follows: The Section 2 provides a review of related studies. In Section 3, an ABAC-MSN model is proposed, with the formal description of the model and its general security rules, and we give some use-case scenarios and relevant policies. The design and implementation of a prototype system based on this model are described in Section 4. Finally, the last section presents the relevant conclusions and work prospects.

2. Related works

Carminati et al. [2] proposed a series of relationship-based access control models (ReBAC), considering the relationship type, relationship depth and trust between users as the main parameters for authorization. In their work, trust values of multiple relationships of the same type on a path can be calculated to form an indirect trust between users that are not directly connected. Fong et al. [8] proposed a Facebook-like access control model, featuring four types of policies that cover four different aspects of access in OSNs, allowing adjustments on user's search, social graph traversal, communication between users and normal user access, but lacking multi-party type and relationship depth. Fong et al. [9], proposed a relationship-based access control model that supports many types of relationships. In addition, Ahn et al. [12] introduced multi-party access control (MPAC), and proposed an MPAC model and multi-party policy specification and the appropriate policy evaluation mechanism.

Cheng et al. [3] proposed a new user-to-user relationship-based access control model (UURAC) that utilizes regular expression notation for policy specification. They developed a path checking algorithm to determine whether the required relationship path between users for a given access request exists, and provided proofs of correctness and complexity analysis for this algorithm. In [4], the author developed an access control model beyond user-to-user (U2U) relationships for OSNs, it incorporates not only U2U relationships but also user-to-resource (U2R) and resource-to-resource (R2R) relationships. Authorization policies were defined in terms of patterns of relationship paths on social graph and the hop count limits of these paths. In [5], an attribute-aware relationship-based access control was proposed, applying attribute-based policies in the UURAC model proposed in [4]. In their work, the worker defined three types of attributes, node attributes, edge attributes and count attributes.

Barbara et al. [1] pointed out that an enhanced social network access control system was the first step to solving the existing online social network security and privacy issues. To address some of the current limitations, they created an experimental social network using synthetic data which they then used to test the efficacy of the semantic reasoning based approaches they had previously suggested. Sachan et al. [15] proposed a fine-grained access control model based on the bit-vector transform domain for MSNs, and verified the security, storage, and execution efficiency of the program through mathematical analysis and simulation experiments.

Given the access control issues of OSNs, Pang et al. [14] summarized and determined new access control requirements in OSNs from the existing access control schemes. From the perspective of user-defined resource access, the researchers focused on public information security of social media. In their work, they proposed a new model for OSNs containing relationships among users and public information. They adopted a mixed logic for the formal description of the access control policies.

In [6], an access control model for MSNs was presented on the basis of the main social relationship attributes of users, including user type, compactness, depth and trust. However, this model lacked multi-attribute support for the platform and ignored user basic attribute, current context information. For trust issues of social media users, Zhang et al. [10, 20, 21] first proposed a within-domain/inter-domain community-based trust evaluation model for MSNs. Through simulation experiments on UCINET social networks, they established a method to enhance or reduce user trust in multimedia content sharing and dissemination.

In summary, current studies on access control for MSNs have mainly focused on the relationship-based access control and considered the social relationship attributes of users, such as relationship type, depth, and trust among users. However, this type of access control lacks support for context information and basic information of user. This paper's purpose is to solve this problem.

3. Establishment and formalization of ABAC-MSN model

3.1 Establishment of ABAC-MSN model

On the MSNs platform, the resource may be provided by users or the administrator. The model describes user's access control in the MSNs. First, a user initiates a session to access another user's resources, the user including access user and resource user, and they all have their own attributes. Once the session has been succeed, the decision model will grant permission to user by compare the access user's attribute based on the policy which is designed by the resource user. Fig. 1 shows a attribute-based access control model for multimedia social networks(ABAC-MSN) and it comprises some basic components: users, sessions, resources, polices and access decision module, as discussed in Section 3.2.

3.2 Definition and formal descriptions of ABAC-MSN model components

Definition 1. (User set, $\mathcal{U}$): User represents the entity that accesses MSNs. In the social networks, the set $\mathcal{U}$ contains all users. The users can upload and access media resources, and perform various operations on other users and resources available in the system. The users can be classified as access user (AU) and resource user (RU). The AU refers to users request access to multimedia resources, while the RU refers to users whose resources are accessed and they have their own authorization policies.

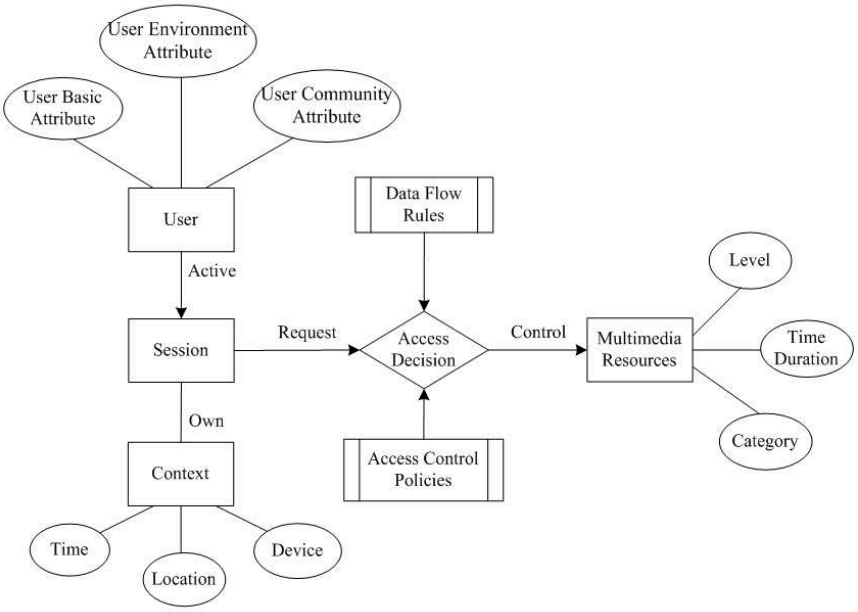

Fig. 1 *Attribute-based access control model for multimedia social networks.*

Definition 2. (User attribute set, $\mathcal{A}_{\mathrm{U}}$): The set $\mathcal{A}_{\mathrm{U}}$ includes user basic information attributes set ($\mathcal{A}_{\mathrm{UB}}$), user social relationships attributes set ($\mathcal{A}_{\mathrm{UR}}$), and user community attributes set ($\mathcal{A}_{\mathrm{UC}}$). The user basic information attributes include a lot of attributes such as name, age, identity, hobbies and user level attributes. The user's social relationships attributes are comprised of relationship type, depth, and compactness attributes. The depth refers to the shortest paths between AU and RU. The compactness refers to the frequency of interaction between users. The user community attributes refer to the community or circle to which users in social networks belong, and users in a community can design different groups, which is an integral part of the entire network relationships.

Definition 3. (Session set, $\mathcal{S}_{\mathrm{e}}$): The set $\mathcal{S}_{\mathrm{e}}$ contains all sessions in an MSNs. A user requests to access multimedia resources and the RU responds according to the attributes of the access user. Once the user receives any requested multimedia resources from a resource user, a session is recorded.

Definition 4. (Environment Attribute set, $\mathcal{A}_{\mathrm{E}}$): The set $\mathcal{A}_{\mathrm{E}}$ contains all environment attributes in a MSNs. The environment attribute refers to the current time, location and the device's information when a user requests to access the resources.

Definition 5. (Access Decision, AD): Access decision refers to a decision module for access authorization, and combining control rules and policy conflict resolution methods, the model makes judgments on users' requests for resource access.

Definition 6. (Multimedia Resources, MMRs): The multimedia resources refer to the media uploaded to a platform by users or the administrator that allows others to access.

Definition 7. (Resource Attributes set, $\mathcal{A}_{\mathrm{R}}$): The set $\mathcal{A}_{\mathrm{R}}$ contains all resources' attributes information. The resource attributes refer to certain features of media resources, which include media level, time duration and category.

Definition 8. (Access Control Policies, ACPs): Access control policies refer to a set of rules for determining whether users have the abilities to access MMRs, thereby restricting the operational behaviors of the subject on the object.

Definition 9. (Operation Permission, OP): The operation permission refers to what kind of operation the user can perform on the multimedia resource. In MSNs, we define the operations of a user on resources are browsing (b), sharing (s'), downloading (d), uploading (u'), commenting (c), tagging (t), and the operation permissions set can be expressed as $\mathcal{P}$=$\{b, s', d, c, u', t\}$. As the symbol $\neg$ represents negation of the permission, for example, the symbol $\neg s'$ indicates that access user is not allowed to share the multimedia resources.

The ABAC–MSN model describes a variety of attributes of MSNs, including certain dynamic attributes, and the granularity refers to the logically dynamic grouping of users. Different attributes depict different granularities by logical operations, such as conjunction $\wedge$, disjunction $\vee$ and negation $\neg$. The access permission involves discrete access control parameters, namely, the requirements of the resource user in the access granularity, and the resource user may customize permission rules according to their needs. The access permission set can be expressed as $\mathcal{L} = \{\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_i, \ldots, \mathcal{L}_n\}$, where $\mathcal{L}_{\mathrm{i}}, i = 1, 2, \ldots, n$, is the element of set $\mathcal{L}$ and n represents the number of access permissions, namely, the resource provider requirements in the access granularity of access users. The access users can design the access permissions of the attributes, and the access user attributes set can be denoted by $\mathcal{A}$=$\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_i, \ldots, \mathcal{A}_n\}$. The logical operation results of $\mathcal{L}$ and $\mathcal{A}$ can be expressed by Q. The Q_{i} represents the logical operation results between the i-the element of $\mathcal{L}$ and $\mathcal{A}$, with the result of 0 or 1. When an attribute corresponding to the access permission has constraints on attribute of user, namely, $\mathcal{A}_i \in \mathcal{L}_i$, we can obtain $Q_{\mathrm{i}} = 1$; otherwise $Q_{\mathrm{i}} = 0$. For the $\wedge$ operation between n access permissions, Q=$Q_1 \wedge Q_2 \wedge \cdots \wedge Q_n$, when $Q = 1$, operation $\mathcal{P}$ is allowed, otherwise denied.

3.3 General constraint rules for MSNs

In general, there are four elements in an access control scenario, a subject, an object, an action, and access control policies. More precisely, the subject tries to perform an action on the object, whether the subject accesses successfully or not depending on the access control rules defined for the subject. In social networks, certain resources may be offered by multiple users. For the sake of simplicity, we assume that the media resources are only owned to a user. Access control rules refer to the requirements in the current attribute while using or sharing multimedia

resources. The users who meet the constraint rules can access multimedia resources, thereby the security of multimedia resources can be guaranteed.

In MSNs, the set $\mathcal{A}_{\mathrm{UB}} = \{name, age, occu, le, h\}$, for $name \in \mathcal{N}$, $age \in \mathcal{A}_{\mathrm{g}}$, $occu \in \mathcal{O}_{\mathrm{c}}$, $le \in \mathcal{L}_{\mathrm{e}}$, $h \in \mathcal{H}$, $\mathcal{A}_{\mathrm{g0}} \in \mathcal{A}_{\mathrm{g}}$. Here we define that $\mathcal{N}, \mathcal{A}_{\mathrm{g}}, \mathcal{O}_{\mathrm{c}}, \mathcal{L}_{\mathrm{e}}, \mathcal{H}$ are user name attributes set, user age attributes set, user occupation attributes set, user level attributes set, user hobby attributes set and the constant quantity are $Name_0, Age_0$, $Occu_0, Le_0$, H_0 respectively.

The set $\mathcal{A}_{\mathrm{UR}}$=$\{rela, dep, comp\}$, for $rela \in \mathcal{R}_{\mathrm{e}}$, $dep \in \mathcal{D}, comp \in \mathcal{C}_{\mathrm{p}}$. And the sets $\mathcal{R}_{\mathrm{e}}$, $\mathcal{D}$, $\mathcal{C}_{\mathrm{p}}$ represent user relationship attributes set, user relation depth attributes set, user compactness attributes set and the constant values are respectively $Rela_0, Dep_0, Comp_0$.

The set $\mathcal{A}_{\mathrm{UC}} = \{comm, g\}$, for $comm \in \mathcal{C}_{\mathrm{m}}, g \in \mathcal{G}$, $\mathcal{G}_0 \in \mathcal{G}$. The sets $\mathcal{C}_{\mathrm{m}}$, $\mathcal{G}$ represent user community attributes set, user group attributes set.

The set $\mathcal{A}_{\mathrm{E}} = \{t, lo, d\}$, for $t \in \mathcal{T}$, $lo \in \mathcal{L}_{\mathrm{o}}$, $d \in \mathcal{D}$, $\mathcal{T}_0 \in \mathcal{T}$. The sets $\mathcal{T}$, $\mathcal{L}_{\mathrm{o}}$, $\mathcal{D}$ respectively represent time attributes set, location attributes set, device attributes set, and the constant values are T_0, Lo_0, D_0 respectively.

Finally, the set $\mathcal{A}_{\mathrm{R}} = \{ca, lev\}$, for $ca \in \mathcal{C}_{\mathrm{a}}, lev \in \mathcal{L}_{\mathrm{ev}}$. The sets $\mathcal{C}_{\mathrm{a}}$, $\mathcal{L}_{\mathrm{ev}}$, represent resource category attributes set, resource level attributes set, and with the constant values of Ca_0 and Lev_0.

The predicate exe is defined as the action taken, and $\mathrm{exe}(u, r, \mathcal{P})$ indicates that the user may access multimedia resources and perform operations described by $\mathcal{P}$.

Rule 1 (Basic Attributes-enabled Constraint Rules)**.** *Access users that have basic information attributes beyond a particular scope don't have permission to access the multimedia resources.*

$$\forall u, name(u \in \mathcal{U}, name \in \mathcal{N})(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\, name(name = Name_0)$$
$$\forall u, age(u \in \mathcal{U}, age \in \mathcal{A}_g)(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\, age(age \in \mathcal{A}_{g0})$$
$$\forall u, occu(u \in \mathcal{U}, occu \in \mathcal{O}_c)(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\, occu(occu = Occu_0)$$
$$\forall u, h(u \in \mathcal{U}, h \in \mathcal{H})(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\, h(h = H_0)$$

Rule 2 (Relationships-enabled Constraint Rules)**.** *Access users that have the social relationships attributes inconsistent with a particular relationship do not have permission to access MMRs.*

$$\forall u, rela(u \in \mathcal{U}, rela \in \mathcal{R}_e)(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ rela(rela = Rela_0)$$
$$\forall u, dep(u \in \mathcal{U}, dep \in \mathcal{D})(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ dep(dep \leq Dep_0)$$
$$\forall u, comp(u \in \mathcal{U}, comp \in \mathcal{C}_p)(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ comp(comp \geq Comp_0)$$
$$\forall u, g(u \in \mathcal{U}, g \in \mathcal{G})(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ g(g \in \mathcal{G}_0)$$

Rule 3 (Environment-enabled Constraint Rules)**.** *The access user invokes the action of the resources in the environment, the user has no permission to access the resource without satisfying a specific value of environment attributes.*

$$\forall u, t(u \in \mathcal{U}, t \in \mathcal{T})(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ t(t \in \mathcal{T}_0)$$
$$\forall u, d(u \in \mathcal{U}, d \in \mathcal{D})(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ dev(d = D_0)$$
$$\forall u, lo(u \in \mathcal{U}, lo \in \mathcal{L}_o)(\mathrm{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ lo(lo = Lo_0)$$

3.4 General data flow rules for MSNs

On MSN platforms, the access user is subject and the MMR is object. The terms $\mathcal{S}$ and $\mathcal{O}$ respectively represent the subject set and the object set. The subject and the object are included in a multimedia system, and they have different levels. For $s \in \mathcal{S}$ and $o \in \mathcal{O}$, a fixed sensitivity levels $T(s)$ and $T(o)$ exist. The security level can form a lattice by relation $\leq$ sorting and security level, but the model may allow lower constraints, as illustrated in Fig. 2.

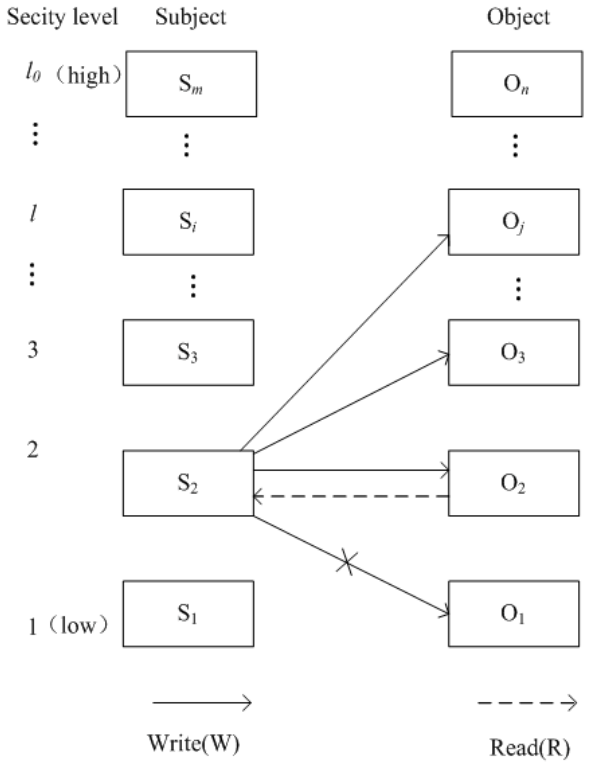

Fig. 2 *Data flow rules for multimedia networks.*

Feature 1. *Only when $T(o) \leq T(s)$ can the subject s has $\mathcal{R}$ operation to access the object o.*

Feature 2. *When $T(o_1) \leq T(o_2)$, s has $\mathcal{R}$ operation on o_1, then s has $\mathcal{W}$ operation on o_2.*

The set $\mathcal{R}$ of user's operation includes browsing, commenting, tagging, and downloading in the MSNs, whereas the set $\mathcal{W}$ represents uploading and sharing. In the MSNs, high-level users may execute $\mathcal{R}$ operations on low-level user's resources. On the contrary, the low-level user can't do $\mathcal{R}$ operations on high-level users. But, Low-level users may perform $\mathcal{W}$ operations on high-level resources.

Rule 4 (Data Flow-enabled Constraint Rules)**.** *Access users whose level lower the resource user's have no permission to access the multimedia resources.*

$$\forall u, le(u \in \mathcal{U}, le \in \mathcal{L}_e)(\text{exe}(u, r, \mathcal{P})) \Rightarrow \exists le(le \geq Le_0)$$

3.5 Policy conflict resolution mechanisms

In the MSNs, a user may not in one group, and a multimedia resource may also belong to more than one category. Thus, these rules may result policy conflicts. To resolve policy conflicts, we adopt simple logic words for logical operations to avoid rule conflicts, such as $\wedge$, $\vee$. If $\wedge$ is applicable, the ACPs are more stringent, and only when all policies are met, then the access permission can be authorized. However, if $\vee$ is applicable, the ACPs are relatively relaxed, and as long as one of the policies is met, the access may be authorized.

User group conflicts. If a user is in the set both $\mathcal{G}_{\text{i}}$ and $\mathcal{G}_{\text{j}}$, for $\mathcal{G}_{\text{i}} \in \mathcal{G}, \mathcal{G}_{\text{j}} \in \mathcal{G}$, $(i, j = 1, 2, \dots)$. A conflict occurs when the resource user restricts users who are in the group $\mathcal{G}_{\text{i}}$ can't be authorized to access, but the user still has permission to access the resource with group $\mathcal{G}_{\text{j}}$. And we provide two rules below for this condition. The access control is relatively strict and the strategy is presented as follows:

$$\forall u, \text{g}(u \in \mathcal{U}, g \in \mathcal{G})(\text{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ g(g \in \mathcal{G}_{\text{i}} \wedge g \in \mathcal{G}_{\text{j}})$$

The access control is relatively relaxed and the policy is written as follows:

$$\forall u, \text{g}(u \in \mathcal{U}, g \in \mathcal{G})(\text{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ g(g \in \mathcal{G}_{\text{i}} \vee g \in \mathcal{G}_{\text{j}})$$

Resource type conflicts. In MSNs, a media is in the both $\mathcal{C}_{\text{ai}}$ and $\mathcal{C}_{\text{aj}}$, for $\mathcal{C}_{\text{ai}} \in \mathcal{C}_{\text{a}}, \mathcal{C}_{\text{aj}} \in \mathcal{C}_{\text{a}}$, $(i, j = 1, 2, \dots)$. A conflict occurs when the resource user restricts the media category in $\mathcal{C}_{\text{ai}}$ can't be accessed, but the user still has permission to access the media in the category $\mathcal{C}_{\text{aj}}$. We provide two rules below for this conflict. The access control is relatively strict and the rule is denoted as follows:

$$\forall u, \text{ca}(u \in \mathcal{U}, ca \in \mathcal{C}_{\text{a}})(\text{exe}(u, r, \mathcal{P})) \Rightarrow \exists\ ca(ca \in \mathcal{C}_{\text{ai}} \wedge ca \in \mathcal{C}_{\text{aj}})$$

The access control is relatively relaxed and the strategy is written as follows:

$$\forall u, \text{ca}(u \in \mathcal{U}, ca \in \mathcal{C}_{\text{a}})(\text{exe}(u, r, \mathcal{P})) \Rightarrow \exists ca(ca \in \mathcal{C}_{\text{ai}} \vee ca \in \mathcal{C}_{\text{aj}})$$

3.6 Access control for use-case scenarios

While setting access control policies, the $\wedge$ or $\vee$ operations between different rules are allowed. Based on the model proposed in this paper and the policy expressions for each of the three scenarios mentioned in Section 1, the ACPs are respectively expressed as follows:

Scenario 1. Alice wanted her friends who have common interest with her to access her multimedia resources. However, for some certain reasons, she did not want Eve to access her contents. To address the problem, the user's basic attributes need to be considered, such as user's name and hobby. At the same time Alice did not allow any of them to download or share her resources. For this use-case scenario, the following policy is proposed:

$$\text{P1:}\langle \mathcal{P} = \{b, \neg s', \neg d, c, u', t\}, (h = \mathsf{travel}) \wedge (rela = \mathsf{friend}) \wedge (name = \neg \mathsf{Eve}) \rangle$$

Scenario 2. Dave is a middle student, we can limit his time spending on the MSNs. First, we can set the user's basic attribute age must be under 18 years old and users under the age are not allowed to share, download the videos. They are allowed to browse, tag, and comment some types of media within a certain period every day. The policy for this scenario is as follows:

$$\text{P2:}\langle \mathcal{P} = \{b, \neg s', \neg d, c, u', t\}, (ca = \mathsf{Ca}_0) \wedge (t \in \mathcal{T}_0) \wedge (age \leq 18) \rangle$$

Scenario 3. If VIP users share their copyrighted medium to non-VIP users, non-VIP users may also access the copyrighted media without appropriate control; thus, the dissemination of the copyrighted media is inefficiently controlled. However, according to the data flow control rules in this paper, Dave can't access any of the videos that Bob shares to him. The policy for this scenario is as follows:

$$\text{P3:}\langle \mathcal{P} = \{b, s', d, c, u', t\}, le_{\text{Dave}} \geq le_{\text{Bob}} \rangle$$

Scenario 4. Charlie allows his friends on the list of his classmates group set ($\mathcal{G}_{\text{classmate}}$) to access his media contents. The policy for this scenario is as follows:

$$\text{P4:}\langle \mathcal{P} = \{b, s', d, c, u', t\}, g \in \mathcal{G}_{\text{classmate}} \rangle$$

However, conflicts may occur while implementing the policies for Eve who is in both classmate group and friend group ($\mathcal{G}_{\text{friend}}$). Based on the conflict resolution methods in this paper, and Charlie strengthen his access control requirements, the policy is as follows:

$$\text{P5:}\langle \mathcal{P} = \{b, s', d, c, u', t\}, (g \in \mathcal{G}_{\text{classmate}}) \wedge (g \in \neg \mathcal{G}_{\text{friend}}) \rangle$$

Thus, Eve can't access Charlie's videos.

4. ABAC-MSN prototype system and its applications

4.1 Design of access control framework

In this paper, the ABAC is implemented on the MSN platform CyVOD (http://www.cyvod.net). The CyVOD platform adopts three-layer B/S architecture, and a hierarchy design method is adopted to implement the system functions. The ABAC-MSN model consists of server, browser (including PC/mobile users), multimedia resources database, user information database and attribute policy database. The specific architectures are shown in Fig. 3 and Fig. 4.

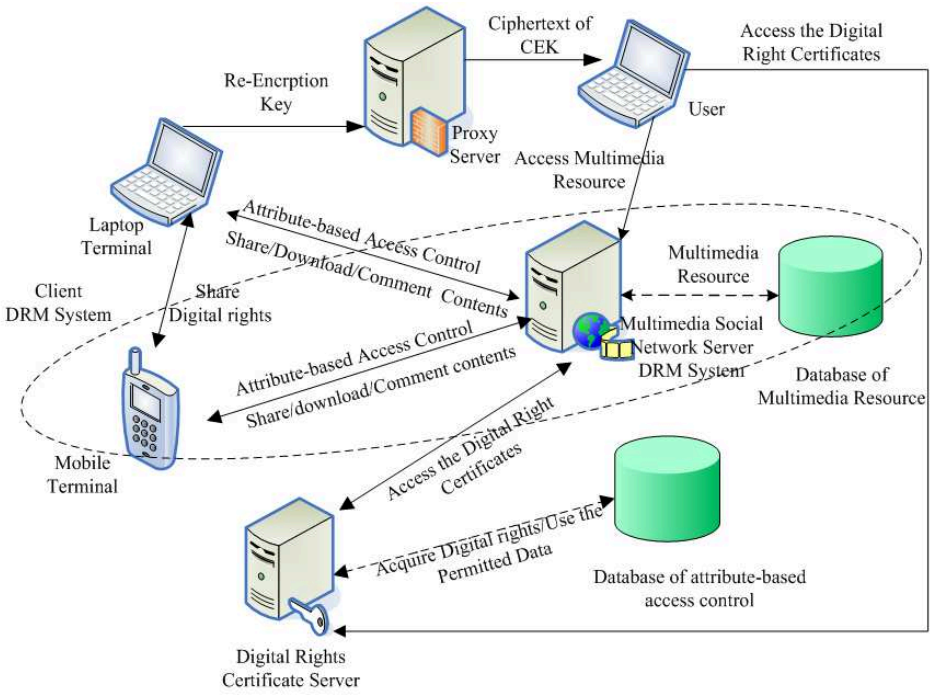

Fig. 3 *The prototype architecture for multimedia social networks.*

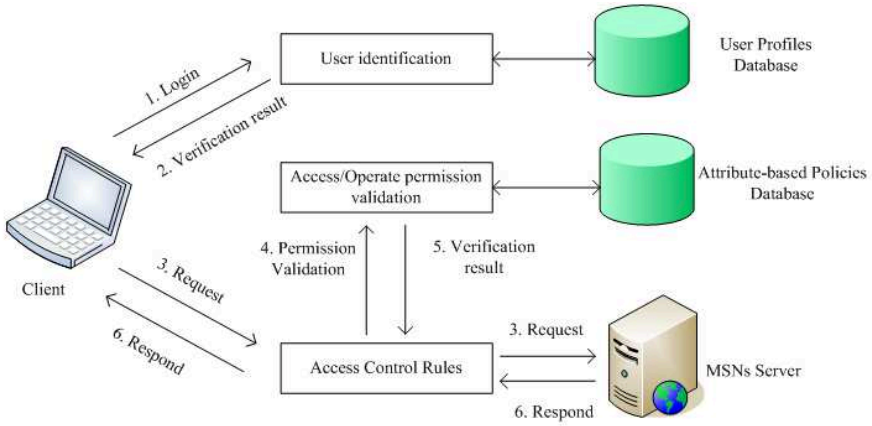

Fig. 4 *Attribute-based access control framework and data flow diagram.*

4.2 Implementation of ABAC-MSN model

After logging in the CyVOD platform, the user can upload multimedia contents and set access permissions for the contents, as illustrated in Fig. 5.

The ABAC-MSN model is implemented on the CyVOD platform, and the constraints on U_{BA} (such as user age, time, user level and Location) are presented in Fig. 6(a), Fig. 6(b), Fig. 6(c), Fig. 6(d) respectively.

Fig. 5 *Multimedia resource authorization on CyVOD.*

4.3 Comparative analysis

The ABAC–MSN access control mechanism proposed in this paper is compared with several social networks access control models [4–6]. The comparative analysis results are shown in Tab. I, where "✓" denotes supporting for the corresponding functions, mechanisms or characteristics, with "×" no supporting.

Cheng et al. [4] proposed the access control mechanism does not take any context information into consideration, and the model does not show any user attribute. The policy language is weak, such as "all friends but Alice may browse the contents", the policy is difficult to express. However, in their work, the relationship-based access control model that incorporates not only U2U relationships but also U2R and R2R relationships, a series of relationships in social networks are considered. Chen et al. [6] proposed an access control model for MSNs, the social relationship attributes of users were considered, such as relationship type, compactness and trust, but lacked of multi-attribute support. Cheng et al. [5] introduced the attribute-based policy language and defined three types of attributes, and the attribute policies were applied to the UURAC model [4], but the context information and resource attributes were not considered.

(a) Age-supported access control.

(b) Time-supported access control.

(c) Level-supported access control.

(d) Localization-supported access control.

Fig. 6 *Attribute-based access control implementation on CyVOD.*

	Cheng [4]	Chen [6]	Cheng [5]	ABAC-MSN
Multi-relationship Types	✓	✓	✓	✓
User Attributes	×	✓	✓	✓
Compactness	✓	✓	✓	✓
U2R relationship	✓	×	×	×
Relationship Depth	✓	✓	✓	✓
Context Information	×	×	×	✓
Historical Behavior	×	✓	×	✓
Resource Attribute	×	×	✓	✓
Policy Conflict Resolution	✓	✓	×	✓

Tab. I *Comparative analysis of access control in social networks.*

5. Conclusions

In this paper, an ABAC model is established by using a variety of attributes for MSNs. The authorization policy takes user attributes, context information and resource attributes into consideration. The definitions of the attributes and the formal description of the model are provided. The attribute policies and policy

conflict resolution mechanisms are established for fine-grained access. Moreover, users can specifically define and control their own operation permissions on the resources. In the future work, we would explore a novel encryption method for user privacy information on the basis of the ABAC–MSN model.

Acknowledgement

We give thanks to the reviewers and editor for their valuable comments, questions, and suggestions. The work was sponsored by National Natural Science Foundation of China Grant No. 61370220, Plan For Scientific Innovation Talent of Henan Province Grant No. 2017JR0011, Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No. 15IRTSTHN010, Program for Henan Province Science and Technology Grant No. 142102210425, Project of the Cultivation Fund of Science and Technology Achievements of Henan University of Science and Technology Grant No. 2015BZCG01.

References

[1] BARBARA C., ELENA F., RAYMOND H., KANTARCIOGLU M. Semantic Web-Based Social Network Access Control. *Computers and Security*. 2011, 30(2), pp. 108–115, doi: 10.1016/j.cose.2010.08.003.

[2] CARMINATI B., FERRARI E., HEATHERLY R., KANTARCIOGLU M., THURAISINGHAM B. Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security*. 2009,13(1), pp. 297–304, doi: 10.1145/1609956.1609962.

[3] CHENG Y., PARK J., SANDHU R. A user-to-user relationship-based access control model for online social networks. In: *Proceedings of the 26th IFIP Annual WG 11.3 Conference on Data and Application Security and Privacy (DBSec 2012)*, Paris, France. 2012, pp. 8–24.

[4] CHENG Y., PARK J., SANDHU R. Relationship-based access control for online social networks: Beyond user-to-user relationships. In: *Proceedings of the 2012 ASE/IEEE International Conference on Social Computing, SocialCom 2012 and the 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT 2012)*, Amsterdam, Netherlands. 2012, pp. 646–655.

[5] CHENG Y., PARK J., SANDHU R. Attribute-aware relationship-based access control for online social networks. In: *Proceedings of the 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec 2014)*, Vienna, Austria. 2014, pp. 292–306.

[6] CHEN Q.L., ZHANG Z.Y., XIANG F., WANG J. Research on the access control model for multimedia social networks. *Journal of Xidian University*. 2014, 41(6), pp. 181–187, doi: 10.3969/j.issn.1001-2400.2014.06.030.

[7] FOGUES R., SUCH J.M., ESPINOSA A., GARCIA F.A. Open Challenges in Relationship-Based Privacy Mechanisms for Social Network Services. *International Journal of Human-Computer Interaction*. 2015, 31(5), pp. 350–370, doi: 10.1080/10447318.2014.1001300.

[8] FONG P.W. Relationship-based access control: protection model and policy language. In: *Proceedings of the 1st ACM Conference on Data and Application Security and Privacy (CODASPY 2011)*, San Antonio, TX, United states. 2011, pp. 191–202.

[9] FONG P.W., SIAHAAN I. Relationship-based access control policies and their policy languages. In: *Proceedings of the 16th ACM symposium on Access control models and technologies (SACMAT 2011)*, Innsbruck, Austria. 2011, pp. 51–60.

[10] FENG W.N., ZHANG Z.Y., WANG J., HAN L.Q. A Novel Authorization Delegation for Multimedia Social Networks by using Proxy Re-encryption. *Multimedia Tools and Applications*. 2016, 75(21), pp. 13995–14014, doi: 10.1007/s11042-015-2929-2.

[11] GAURAV M., SUCH.J.M. How socially aware are social media privacy controls. *IEEE computer society*. 2016, 49(3), pp. 96–99, doi: 10.1109/mc.2016.83.

[12] HU H.X., AHN G.J., JORGENSEN J. Multiparty access control for online social networks: Model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*. 2013. 25(7), pp. 1614–1627, doi: 10.1109/TKDE.2012.97.

[13] MEO P.D., FERRARA E., ROSACI D., SARNE G.M.L. Trust and Compactness in Social Network Groups. *IEEE Transaction on Cybernetics*. 2015, 45(2), pp. 205–216, doi: 10.1109/TCYB.2014.2323892.

[14] PANG J., ZHANG Y. A new access control scheme for Facebook-style social networks. *Computers and Security*. 2015, (54), pp. 44–59, doi: 10.1016/j.cose.2015.04.013.

[15] SACHAN A., EMMANUEL S., KANKANHALLI M. An Efficient Access Control Method for Multimedia Social Networks. In: *Proceedings of the 2nd ACM SIGMM Workshop on Social Media*, Firenze, Italy. 2010, pp. 33–38.

[16] ZHANG Z.Y., GUPTA B.B. Social Media Trustworthiness and Security: Overview and New Direction. *Future Generation Computer Systems*. 2016, pp. 1–12, doi: 10.1016/j.future.2016.10.007.

[17] ZHANG Z.Y. Digital Rights Management Ecosystem and its Usage Controls: A Survey. *International Journal of Digital Content Technology and Its Applications*. 2011, 5(3), pp. 255–272, doi: 10.4156/jdcta.vol5.issue3.26.

[18] ZHANG Z.Y., WANG Z., NIU D. A Novel Approach to Rights Sharing-Enabling Digital Rights Management for Mobile Multimedia. *Multimedia Tools and Applications*. 2015, 74(16), pp. 6255–6271, doi: 10.1007/s11042-014-2135-7.

[19] ZHANG Z.Y. Security, Trust and Risk in Multimedia Social Networks. *The Computer Journal*. 2015, 58(4), pp. 515–517, doi: 10.1093/comjnl/bxu151.

[20] ZHANG Z.Y., WANG K.L. A Trust Model for Multimedia Social Networks. *Social Networks Analysis and Mining*. 2013, 3(4), pp. 969–979, doi: 10.1007/s13278-012-0078-4.

[21] ZHANG Z.Y., ZHAO C.W., WANG J. *Social Media Networks Security Theory and Technology*. Beijing: Science Press, 2016.