

在线社交网络中延伸访问控制机制研究

谢绒娜, 范晓楠, 袁琳, 郭子晨, 朱家玉, 史国振

(北京电子科技学院密码与科学技术系, 北京 100070)

摘要: 针对社交网络中用户发布的数据延伸不可控的问题, 提出了一种基于隐私标签的延伸控制机制。该机制基于用户关系跳数和资源转发跳数给用户和数据分配不同类型的隐私标签, 以实现数据的细粒度延伸访问控制。提出了隐私标签的生成算法和分配方法, 设计了隐私标签约束规则并对可能出现的策略冲突进行分析。最后通过测试, 表明了该机制可以实现社交网络中细粒度延伸控制, 同时证明了该机制的安全性和有效性。

关键词: 在线社交网络; 隐私标签; 延伸控制; 隐私保护; 信息安全

中图分类号: TP302

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021075

Research on extended access control mechanism in online social network

XIE Rongna, FAN Xiaonan, YUAN Lin, GUO Zichen, ZHU Jiayu, SHI Guozhen

Department of Cryptography and Science Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Aiming at the problem of inability to extend control over the data published by users in social networks, an extended access mechanism based on privacy labels was proposed. This mechanism granted users and data different types of labels based on the number of user relationship hops and resource forwarding hops, so as to achieve fine-grained extended access control to the data. The generation algorithm and distribution method of privacy labels were proposed. The constraint rules of privacy label were designed and the possible policy conflicts were analyzed. Finally, the test proves that the mechanism achieves fine-grained extended control in social networks, and proves its security and validity of the mechanism.

Keywords: online social network, privacy label, extended control, privacy protection, information security

收稿日期: 2020-12-08; 修回日期: 2021-03-23

通信作者: 史国振, sgz1974@163.com

基金项目: 国家重点研发计划(2017YFB0802705); 国家自然科学基金(61932015)

Foundation Items: The National Key R&D Program of China (2017YFB0802705), The National Natural Science Foundation of China (61932015)

论文引用格式: 谢绒娜, 范晓楠, 袁琳, 等. 在线社交网络中延伸访问控制机制研究[J]. 网络与信息安全学报, 2021, 7(5): 123-131.

XIE R N, FAN X N, YUAN L, et al. Research on extended access control mechanism in online social network[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 123-131.

1 引言

随着智能手机、平板电脑等移动终端的普及,在线社交网络(OSN, online social network)已经成为人们交往互动的重要平台,如国内的微信、微博,国外的 Facebook 等。人们享受着社交网络提供的各种个性化服务的同时面临着隐私泄露的问题。对于自己发布的信息,用户无法完全控制其传播路径,一旦信息被不良用户获得,可能被恶意利用,造成严重后果。

访问控制机制能够有效防止个人信息被不信任的请求者获取而加以利用。基于角色的访问控制(RBAC, role based access control)模型^[1]是社交网络中常用的访问控制模型之一,其核心是将用户分成不同的角色,然后赋予角色一定的权限,但具有访问控制粒度较粗、缺乏灵活性的缺点。文献[2]根据社交网络中用户之间的关系类型、深度等要素,提出了基于关系的访问控制模型。对于基于关系的访问控制模型,后续不少研究通过引入信任值等要素表示关系的强弱来进一步实现细粒度的访问控制。但对于资源离开所有者后进一步的延伸控制问题考虑很少。

为解决社交网络中数据离开所有者进一步的延伸访问控制问题,本文提出了一种基于隐私标签的访问控制(PLBAC, privacy label based access control)机制。本文的主要贡献如下。

(1) 提出了基于隐私标签的访问控制机制,基于用户关系跳数和资源转发跳数给用户和资源分配不同的隐私标签,实现社交网络中资源的延伸控制。

(2) 制定了隐私标签的约束规则,对可能出现的策略冲突情况进行了分析。

(3) 对基于隐私标签的延伸访问控制机制进行了测试,证明了本文提出的机制的安全性和有效性。

2 相关工作

目前,国内外很多学者都在隐私保护的问题上做出了贡献,在 OSN 的实际应用中,人们期望它能够提供更真实的个人信息,且交友模式建立在现实生活中的社交圈,这便产生了基于关系的访问控制机制^[3]。Gates 等^[2]最先提出的基于关

系的访问控制,将关系类型和关系层次作为判断客体访问权限的要素。Fong^[4]将基于关系的访问控制模型发展为一种通用的访问控制范例,文献[5]将其应用到医疗病例系统,解决了传统的基于角色医疗病例系统不够精细的问题。Guo 等^[6]提出了一种基于信任度的隐私保护的好友推荐的方法,支持用户根据自己的隐私偏好找到匹配的好友并与之建立社交关系。Cheng 等^[7]提出了一种基于用户关系的访问控制模型,利用正则表达式描述策略,并提出了一种路径检测方法来判断满足指定关系的所有关系路径。

基于属性的访问控制综合各种属性因素作为授权决策的依据,将访问请求者和资源具有的属性通过特性来标识,扩展性较强,常与其他模型结合使用,这使访问控制过程更加安全。Cheng 等^[8]将属性条件加入基于关系的访问控制模型中,在关系的基础上考虑属性的因素,使访问控制模型更加细粒度。Li 等^[9]提出了一种基于传播链的访问控制模型,允许传播链上的用户按先后顺序为图片设置策略,限制后续用户的操作权限和可赋予权限,但没有给出延伸控制形式化的定义。

“安全标签”的概念最早由强制访问控制(MAC)中的 BLP 模型提出,但标签只是针对等级比较的标识,并不适用于在线社交网络的场景中。之后 IBM 也将标签运用到数据库的保护中。基于标签的访问控制,旨在通过对标签的管理达到访问决策的目标,本文借用标签的含义,提供一种适用于在线社交网络的访问控制方案。

3 社交网络应用场景

本节先对社交网络中数据的流转场景进行分析,再通过社交网络图的形式呈现用户在社交网络环境中拥有的社会关系。

3.1 数据流转场景分析

社交网络中用户关系分为直接关系和间接关系,用户以一定的线下交友为基础,通过一些社交平台不断地以 Friend of Friend^[10]的方式连接在一起,构成了庞大的社交网络,如图 1 所示。用户之间通过交互,可能使原本是间接关系的用户变成具有直接关系的好友,使单独的用户加入各种不同的用户

群组，使不同社交平台的用户联系在一起。

社交网络的开放性和动态性使资源数据可以在不同的用户、用户组以及社交平台间流转，但也正因为这种开放性和动态性，用户发布的个人信息在流转过程中具有相对的不可控性。以微信平台为例，用户在微信中可以添加多个好友并根据社交需要加入各种群组，随着好友数量的增加，用户在分享朋友圈时会考虑哪些人可见哪些不可见，此时用户可以对好友进行分组，设置内容分组可见。假设用户A在微信朋友圈发布了一张生活照片，之后有访问权限的好友可能会对照片进行查看、点赞、评论，还可能会下载照片然后分享给微信中其他原本不被授权的用户或群组，甚至分享到微博、Facebook等社交平台，这使原本不被授权的用户有可能获取到用户A的照片，从而造成用户A的隐私泄露。

通过对资源数据在社交网络中流转场景的分析可知，用户分享的资源数据被授权用户获取后的隐私性是无法保障的。如何对资源进行细粒度的访问控制以及对被好友获取到的数据进行延伸控制是本文研究的主要内容。

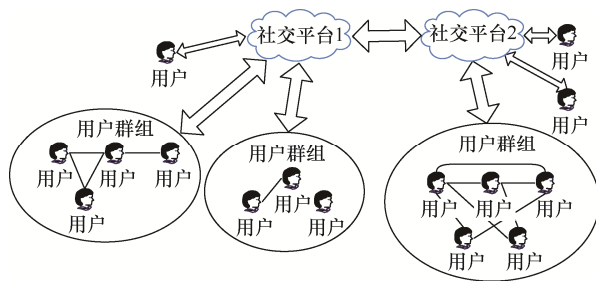


图1 社交网络应用场景
Figure 1 Social network application scenario

3.2 社交网络图

社交网络中维系着大量复杂的用户关系，社交网络可抽象为由不同用户及对应社交关系所组成的网络拓扑^[1]。本文采用社交网络图对社交网络中维系着的各种用户关系及属性进行更直观地表示，如图2所示。图2的节点表示用户，如图中A、B、C；每条边对应一种关系类型和对应节点的亲密度，且两个亲密度中前者对应靠左的节点，如图中节点A、B间的边对应的(f,d7,d5)表示用户A与B为朋友关系，且B对于A来说亲密度为d7，A对于B来说亲密度为d5。关系类型包括f、c、r，分别代表朋友（friend）、同事

（colleague）、亲戚（relative）关系，亲密度由用户根据实际情况设定。同时用户不仅以个人的形式存在于在线社交网络中，而且基于固定属性或上下文的一类用户属于一个用户组中，图2的虚线内表示一个用户组。

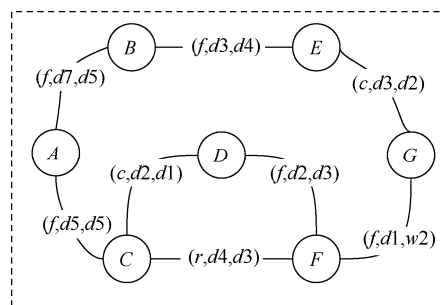


图2 社交网络图
Figure 2 Social network diagram

4 基于隐私标签的访问控制机制

通过社交网络图描述明确了需要考虑到访问控制因素，本节将从访问控制模型、隐私标签的管理、隐私标签的约束规则以及规则冲突解决方面对基于隐私标签的访问控制机制进行详细阐述。

4.1 基于隐私标签的访问控制模型

对基于隐私标签的访问控制模型组件的定义以及具体结构进行说明。

定义1 用户（U，User）：社交网络中已经注册的一组对象请求者。 U 表示社交网络中用户的集合， u_i 表示集合中的用户， $U = \{u_1, u_2, u_3, \dots, u_n\}$ 。例如，图2的用户集合 $U = \{A, B, C, D, E, F, G\}$ 。

用户分为资源用户（RU）和访问用户（AU）。资源用户是最初拥有资源的用户，处于传播过程中的起始用户，具有最高的访问权限。访问用户是指资源传播过程中试图访问资源的用户。

定义2 客体（Object，O）：社交网络中用户依据权限访问的资源。 O 表示社交网络中资源的集合， o_i 表示集合中的资源， $O = \{o_1, o_2, o_3, \dots, o_n\}$ 。资源类型广泛，包括文本、图片、视频等。

定义3 隐私标签（PL，privacy label）：包括主体标签（SL，subject label）和客体标签（OL，object label）两大类。主体标签为用户加入社交网络时，系统根据社交网络图中用户关系为用户分配

的一组隐私标签。客体标签为用户创建客体时为客体分配的一组隐私标签。主体对客体的访问权限由主体和客体对应的隐私标签来决定。PL 表示社交网络中隐私标签的集合, pl_i 表示集合中的一种隐私标签, $PL = \{pl_1, pl_2, pl_3, \dots, pl_n\}$ 。

定义 4 主体标签: 系统为用户分配的一组标签, 由用户的某些属性组成, 具体包括用户的所属用户组属性、用户社会关系属性、跳数属性。

用户组属性即用户所属的群组。用户社会关系属性包括用户在社交网络中的信任水平、用户之间的关系类型以及亲密程度。跳数属性指访问用户和资源用户的关系跳数, 由系统根据社交图查找最短路径得到。例如, 假设图 2 中的 A 为资源用户, 则用户 D 的跳数为 2。

定义 5 客体标签: 资源用户为资源制定的标签, 由资源的隐私水平属性以及规定的用户属性组成。

规定的用户属性包括用户组属性、用户社会关系属性以及跳数属性。其中用户组属性、用户社会关系属性的含义与主体标签相同。跳数属性包括资源用户允许访问者和他的关系跳数上限与及资源转发跳数上限两部分。

定义 6 操作 (AC, action): 在社交网络中访问用户可以对目标资源执行的一系列操作, 常用操作有读取 (r, read)、下载 (d, download)、评论 (c, comment)、转发 (s, share)、修改 (e, edit) 等。

定义 7 访问控制策略 (P, access control policy): 确定请求者是否有权访问资源的规则约束集合, 限制了主体对客体进行相应操作的权限。

在基于隐私标签的访问控制模型中, 首先为主体和客体分别分配隐私标签; 然后系统根据标签信息, 查找对应的访问控制策略, 对访问用户提交的请求进行访问控制决策; 最后执行决策结果, 结果表现为允许访问或拒绝操作。模型结构如图 3 所示。

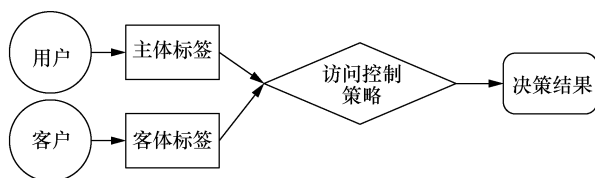


图 3 模型结构
Figure 3 Model structure

4.2 隐私标签概述

基于隐私标签的访问控制是以隐私标签作为访问控制的载体, 通过一定的访问控制策略对隐私标签之间进行比较, 从而进行访问授权。本节对隐私标签的分类、生成、存储以及分配做出详细说明。

4.2.1 标签的分类

基于隐私标签的访问控制模型中的标签分为主体标签和客体标签两大类, 每类标签都是一组标签的集合, 考虑到社交网络环境中的隐私保护要求, 主体标签和客体标签具体由以下 3 种标签构成。

(1) 用户标签 (UL, user label)

由图 2 可知, 用户在社交网络中会涉及其所在的用户组、社交关系以及在社交网络图中的跳数等属性。为资源和用户分配用户标签, 是为了使资源数据以资源所有者的意愿在社交网络中进行传播。

用户的用户标签包括用户组 (UL_group)、用户关系 (relative_type)、与资源用户的关系跳数 (count_r) 3 种属性, 如图 4 所示。其中关系跳数是由系统根据社交图查找最短路径得到的, 当访问用户请求访问资源时, 系统会以资源用户为起点, 寻找访问用户可经历的最短路径, 赋予当前访问用户关系跳数属性。

资源的用户标签规定了访问用户需满足的用户条件, 包括用户组、用户关系、允许访问的关系跳数以及资源转发跳数 (count_s) 4 种属性, 如图 4 所示。

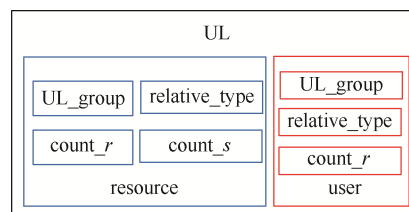


图 4 用户标签组成
Figure 4 User label composition

(2) 隐私强度标签 (PIL, privacy intensity label)

对资源来说, 隐私强度越高代表资源的保密性越强, 对于用户的信任级别要求越高。对用户而言, 隐私强度标签代表用户的信任程度, 信任程度越高的用户在一定条件下越容易得到访问资源的权限。

如图 5 所示, 资源的隐私强度标签包括资源

的隐私水平 (PIL_privacy); 用户的隐私强度标签包括用户的信任水平 (PIL_trust) 及其与资源用户的亲密度 (PIL_close)。

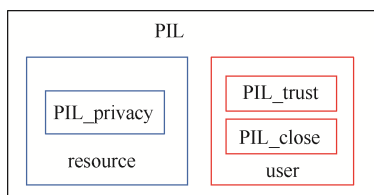


图 5 隐私强度标签组成

Figure 5 Privacy intensity label composition

(3) 环境标签 (EL, environment label)

环境标签包括时间 (time) 和地点 (location) 两个属性, 如图 6 所示。资源的环境标签表示该资源允许用户访问的时间和地点范围, 用户的环境标签表示用户所处时间和地点。

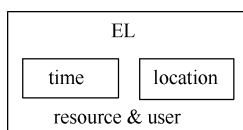


图 6 环境标签组成

Figure 6 Environment label composition

4.2.2 标签的管理

标签的管理指标签的生成、存储以及分配过程。

由 4.2.1 节可知, 主体标签和客体标签均由 3 类标签组成, 每一类标签都有固定的属性信息。因此按照标签生成算法 CreateLabel, 提取标签所涉及的每一类属性信息按照已知的编码规则进行编码, 可采用纠错一位的汉明码进行编码校验; 之后采用加密算法对标签进行加密处理, 形成最终的标签信息, 保证隐私标签在社交网络中的传播过程中的完整性^[12]。标签生成如算法 1 所示。

算法 1 CreateLabel

输入 原始属性信息 raw

输出 资源标签 label

(information collecting phase) // 信息提取阶段

if (raw != null) THEN // raw 为原始添加的属性信息

// 按照已知的编码规则进行编码

code according to coding rules

else

goto the first step // 返回第一步

(label encryption phase) // 标签加密阶段

encrypt with encryption algorithm // 使用加密算法进行加密

(result generation phase) // 结果生成阶段

return label // label 为最终的标签信息

按照上述标签生成算法生成标签后对标签进行分配操作。

定义 8 $\text{allot_pl}_i(u_i)$ ($\text{pl}_i \in \text{PL}$, $u_i \in U$) 表示社交网络中为用户 u_i 分配隐私标签的操作。当用户请求添加好友时, 确定用户被成功添加后系统执行 $\text{allot_pl}_i(u_i)$ 操作, 并为其分配合适的隐私标签; 通过执行 $\text{allot_pl}_i(u_i)$ 可以更新用户隐私标签。

定义 9 $\text{allot_pl}_i(o_i)$ ($\text{pl}_i \in \text{PL}$, $o_i \in U$) 表示社交网络中为客体 o_i 分配隐私标签的操作。当用户创建新的客体时, 客体成功创建后执行 $\text{allot_pl}_i(o_i)$ 操作, 并为其分配隐私标签; 执行 $\text{allot_pl}_i(o_i)$ 操作可以用来更新客体隐私标签。

对于客体标签, 采用粘性策略将客体与隐私标签进行一起绑定传播。例如, 对于 JPEG 格式图片来说, 元数据是以 exchangeable image file (EXIF) 信息存储的, 因此将隐私标签嵌入 EXIF 结构中, 这样隐私标签可以随图片在社交网络中流动, 并且隐私标签的嵌入不会影响图片的正常显示。

主体标签存储在数据库中, 主要包括 6 种数据表。

(1) 用户表 user_table 。存储主体用户的基本信息包括用户 ID、用户名、用户所属用户组、用户的其他信息。具体字段信息定义如下: $\text{user_table}(\text{user_id}, \text{user_name}, \text{user_group}, \text{user_other})$ 。当用户第一次访问数据库时, 需要向数据库提交注册信息, 只有用户表中登记过的用户才能被进一步授予权限。

(2) 好友信息表 relative_table 。存储主体用户的好友信息包括好友 ID、好友用户名、好友关系类型、好友所属用户组、好友其他信息。具体字段信息定义如下: $\text{relative_table}(\text{relative_id}, \text{relative_name}, \text{relative_type}, \text{relative_group}, \text{relative_other})$ 。

(3) 隐私标签表 label_table 。存储隐私标签

的基本信息包括隐私标签 ID、隐私标签名称。具体字段信息定义如下：lable_table (label_id, label_name)。

(4) 用户标签信息表 UL_table。存储用户标签的基本信息包括好友 ID、隐私标签 ID、用户组、关系类型、与资源用户的关系跳数。具体字段信息定义如下：UL_table(relative_id, label_id, UL_group, relative_type, count_r)。

(5) 隐私强度标签信息表 PIL_table。存储隐私强度标签的基本信息包括好友 ID、隐私标签 ID、信任水平、与资源用户的亲密度、具体字段信息定义如下：PIL_table(relative_id, label_id, PIL_trust, PIL_close)。

(6) 环境标签信息表 EL_table。存储环境标签的基本信息包括好友 ID、隐私标签 ID、时间、地理位置。具体字段信息定义如下：EL_table(relative_id, label_id, EL_time, EL_loc)。

4.3 隐私标签的约束规则

PLBAC 授权模型表示为四元组：(SL, OL, AC, P)。其中，SL 表示主体标签，OL 表示客体标签，AC 为操作方式，P 为访问控制策略。基于标签访问控制模型的函数关系可以表示为

$$f: SL \oplus OL \oplus AC \oplus PLBAC_Policy = \{true, false\}$$

该函数表述了 PLBAC 模型基于用户和资源的隐私标签和访问控制策略进行访问授权判断。其中，访问控制策略为与主体标签和客体标签对应的约束规则，下面对 3 种隐私标签对应的约束规则进行详细介绍。

4.3.1 用户标签约束规则

制定用户标签的目的是细粒度的控制访问用户满足的条件。为了进行延伸控制，引入了跳数的概念，关系跳数决定着可以访问的用户与资源用户所处关系网需满足的最大深度，转发跳数决定着资源的转发次数。

资源的用户标签分别用 $UL_g(o_i)$ 、 $UL_e(o_i)$ 、 $count_r(o_i)$ 、 $count_s(o_i)$ 表示规定的用户组属性、关系类型、关系跳数上限以及资源转发跳数上限。用户的用户标签分别用 $UL_g(u_i)$ 、 $UL_e(u_i)$ 、 $count_r(u_i)$ 表示用户所在用户组、与资源用户具有的关系类型、与资源用户的关系跳数。

当用户 u_i 要求对资源 o_i 进行访问时，系统提取上述信息并根据以下访问控制策略规则做出判断。

规则 1 若 $UL_g(o_i) = \{g_1 \cup g_2 \cup \dots \cup g_n\}$ ，当且仅当 $UL_g(o_i) \cap UL_g(u_i) \neq \emptyset$ 时，用户满足所在用户组要求。

若 $UL_g(o_i) = \{g_1 \cap g_2 \cap \dots \cap g_n\}$ ，当且仅当 $UL_g(o_i) \subseteq UL_g(u_i)$ 时，用户满足所在用户组要求。

规则 2 当且仅当 $UL_e(u_i) \subseteq UL_e(o_i)$ 时，访问用户满足资源用户规定的用户关系要求。

规则 3 当且仅当 $count_r(u_i) \leq count_r(o_i)$ 时，访问用户满足与资源用户关系跳数的要求。

规则 4 资源每进行一次转发，执行 $count_s(o_i)$ 。当且仅当 $count_s(o_i) > 0$ ，即资源的转发跳数大于 0 时，访问用户在满足其他条件的同时才可以执行转发操作。

4.3.2 隐私强度标签约束规则

将用户对于资源的访问按操作等级分为 3 类：“读取”功能属于基本操作，为第一类操作等级，记为 r ；“评论”“转发”功能属于第二类操作等级，记为 s ；“下载”“修改”功能属于第三类操作等级，记为 e 。3 类操作等级满足 $r < s < e$ 。

用户的隐私强度标签分别用 $PIL_t(u_i)$ 、 $PIL_c(u_i)$ 表示用户 u_i 的信任水平及其与资源用户的亲密度，其中用户 u_i 的信任水平由系统根据社交网络中其他用户对 u_i 的综合评价来判定，用户 u_i 与资源用户的亲密度由资源用户决定。 $PIL(o_i)$ 表示资源数据 o_i 的隐私强度标签中的隐私水平内容，即 o_i 的隐私水平等级。

当用户 u_i 要求对资源进行访问时，若用户满足用户标签约束规则，系统会提取上述隐私强度标签信息，并根据以下访问控制规则做进一步判断。

规则 5 当且仅当 $PIL_t(u_i) > PIL(o_i)$ ，即用户的信任水平高于资源的隐私水平时，用户才具有对资源进行访问的权限。

规则 6 当 $PIL_t(u_i) > PIL(o_i)$ 时，若 $PIL_c(u_i) \geq r$ ，则允许 u_i 对 o_i 执行第一类操作；若 $PIL_c(u_i) \geq s$ ，则允许 u_i 对 o_i 执行第二类操作；若 $PIL_c(u_i) \geq e$ ，则允许 u_i 对 o_i 执行第三类操作。

4.3.3 环境标签 (EL) 约束规则

用户的环境标签分别用 $T(u_i)$ 、 $Loc(u_i)$ 表示

用户 u_i 的访问时间和访问位置。资源的环境标签分别用 $T(o_i)$ 、 $Loc(o_i)$ 表示允许用户访问资源 o_i 的时间和位置。环境标签中时间和位置均可以为单值、多值或区间，时间由系统时间决定，位置由系统定位决定。若时间范围从 t_i 开始到 t_j 结束，则这段时间表示为 $t_L = t_i \rightarrow t_j (i \leq j)$ 。若地理位置范围从 loc_i 开始到 loc_j 结束，则这段地理位置表示为 $loc_L = loc_i \rightarrow loc_j (i \leq j)$ 。

当用户 u_i 要求对资源 o_i 进行访问时，若满足用户标签和隐私强度标签约束规则，系统会提取环境标签信息并根据以下访问控制规则继续判断，若同样都满足，则最终判定允许用户 u_i 对资源 o_i 进行某种操作，否则拒绝。

规则 7 当且仅当 $T(u_i) \subseteq T(o_i)$ 时，访问用户满足时间要求。

规则 8 当且仅当 $Loc(u_i) \subseteq Loc(o_i)$ 时，访问用户满足位置要求。

通过对 3 类标签的描述，可以对客体标签和主体标签进行符号定义如下。

客体标签 OL 定义为： $OL = \langle (UL_g, UL_e, count_r, count_s), (IPL), (t, loc) \rangle$ 。

主体标签 SL 定义为： $SL = \langle (UL_g, UL_e, count_r), (IPL_t, IPL_c), (t, loc) \rangle$ 。

4.4 策略冲突类型

资源在多个用户间传播时，很可能发生策略冲突问题，本节分析可能发生隐私策略冲突并提出解决的方法。

(1) 对共同好友的隐私策略不同造成的冲突。假如用户 A 在自己的社交网络平台上分享了一幅图片，且设置关系跳数为 2。若根据访问控制规则判定其好友 B 拥有转发权限，B 转发后判断 B 的好友 C 也具有访问权限，但如果 C 同时是 A 的好友，且根据 A 对 C 设置的隐私标签判断 C 不能对图片进行访问，此时就产生了隐私策略冲突。

(2) 共同所有者隐私策略不同造成的冲突。假如一幅图片是用户 A 与用户 B 的合照，那么这幅图片同时属于这两个人，此时一方的操作很可能泄露另一方的信息。D 既是 A 的好友也是 B 的好友，若 A 和 B 对 D 设置的隐私标签决策结果不同，那么就会发生隐私策略冲突。

对于第一种情形，如果资源所有者拒绝了特定用户的访问，即使后面有人授予该用户访问的权限，也以资源所有者的决策为准，即判定拒绝访问。对于第二种情形，资源共有者中假如一方拒绝特定用户的访问，即判定拒绝访问。

5 基于隐私标签的访问控制机制的测试

在社交网络中，用户常通过分享图片进行社交活动，照片受控共享已成为社交网络中隐私保护需考虑的核心问题之一^[13]。借鉴 Karjoth 等^[14]提出的粘性策略 (sticky policy) 思想，针对 JPEG 格式的图片，基于 EXIF 元数据实现隐私标签的嵌入。元数据是指描述文件属性的数据，常见的元数据包括 3 种：EXIF、IPTC 和 XMP^[15]。EXIF 数据一般嵌入图像文件中，不会因图片传播而丢失。

下面基于图 2 的社交网络图中的社会关系，介绍本文提出的基于标签的访问控制机制如何进行访问授权。假设，用户 A 发布了图片 a，并希望只有用户组 g_1 、 g_2 中具有朋友关系的用户可以进行一定的操作。

按照隐私需求，用户 A 在发布图片时为其设置标签 $OL_a = \langle (g_1 \cup g_2, f, 2, 1), (13), (t_i \rightarrow t_j, null) \rangle$ ，并通过 SetLabelValues 将标签存储到 JPEG 结构中的 EXIF Sub IFD^[16]下自定义的结构 Policy IFD 中，存储内容如表 1 所示。

表 1 Policy IFD 中存储的隐私标签内容
Table 1 Privacy label content stored in Policy IFD

隐私标签	说明
public final static int Privacylevel=0x0001	图片的隐私水平
public final static int Actionlevel=0x0002	图片的操作类型
public final static int Relativelevel=0x0003	用户的信任度
public final static int Group=0x0004	用户组
public final static int Relative=0x0005	用户关系
public final static int Count_r=0x0006	关系跳数
public final static int Count_s=0x0007	转发跳数
public final static int Time=0x0008	时间
public final static int Location=0x0009	地理位置

系统为社交网络图中的用户分配标签并存储到数据库中，如用户 B 的标签为 $SL_B = \langle (g_1, f, 1)$,

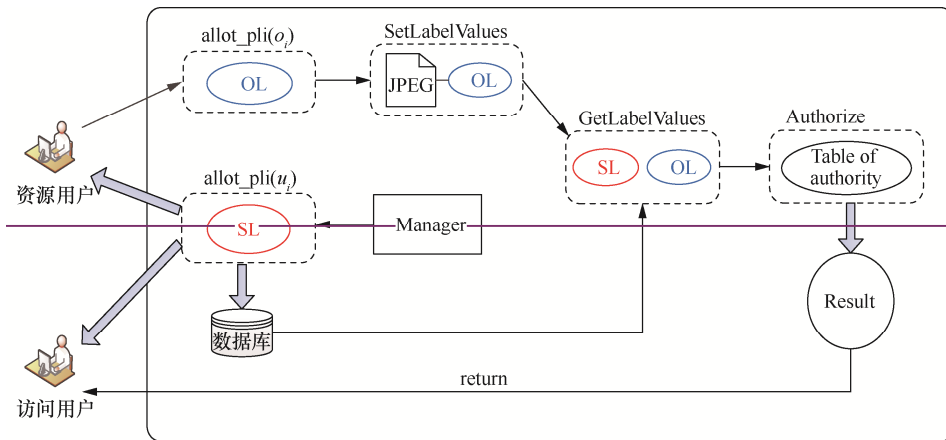


图 7 访问控制过程示例
Figure 7 Example of access control process

$(t4, d7), (t_a, \text{null}) >$, 其中 $i < a < j, d7 > e$ 。用户 E 的标签为 $SL_E = \langle (g_2, f, 2)(t2, d3), (t_b, \text{null}) \rangle$, 其中 $i < b < j, r < d3 < s$ 。假设用户 B 请求访问图片 a, 则系统通过 GetLabelValues 获取用户 B 和图片 a 的标签信息, 再根据标签的约束规则进行授权决策, 用户 B 所属用户组为 g_2 满足所在用户组要求, 与用户 A 的关系为朋友且关系跳数为 1, 满足用户标签约束规则。又有 B 的信任水平 $t4$ 大于资源的隐私水平 $l3$, 同时 B 与 A 的亲密度高于第三类操作等级, 且环境标签信息满足规定, 因此判断用户 B 对 A 的资源具有第三类操作权限, 当然也可以进行第一、二类操作。最后将结果返回给访问用户 B, 整个访问控制过程如图 7 所示。

假设 B 按照所获取的权限对照片 a 进行了转发操作, 则照片 a 的标签更新为 $OL_a = \langle (g_1 \cup g_2, f, 2, 0), (l3), (t_i \rightarrow t_j, \text{null}) \rangle$ 。此时若用户 E 提出访问请求, 则按照图 7 中的流程将用户 E 的标签与更新后的资源标签进行比较, 首先用户 E 所属用户组为 g_2 满足所在用户组要求, 与用户 A 的关系为朋友且关系跳数为 2, 满足用户标签约束规则, 但此时图片 a 的转发跳数为 0, 故 E 不能再对其进行转发。又由于用户 E 的信任水平为 $t2$ 小于资源的隐私水平 $l3$, 故用户 E 也没有读取权限。

本文将访问规则通过中间件的形式对上述示例进行测试, 本文提出的基于标签的访问控制机制通过对比隐私标签进行访问授权, 实现了对资源的延伸控制, 达到了预期效果, 证明了所提方

案的有效性。

6 结束语

针对社交网络中用户发布的信息被授权用户获取后无法保障其隐私性的问题, 以基于关系和属性的访问控制模型为基础, 提出了基于隐私标签的延伸访问控制机制。通过加入用户关系跳数和资源转发跳数解决资源在流转过程中的延伸授权问题, 规定跳数内满足一定条件的用户可以对资源进行访问。通过授予用户和资源 3 种类型的隐私标签来实现对资源较细粒度的访问控制。对隐私标签的分类、生成、存储以及分配做出详细说明, 同时在此基础上制定了相关约束规则, 并对可能出现的策略冲突情况以及解决方法进行了说明。以 JPEG 格式的图片为例对基于隐私标签的延伸访问控制机制进行测试, 证明了本文提出的理论和方法在隐私保护方面的合理性和有效性。

本文测试部分选择的图片场景不能代表所有系统中的情况, 下一步工作将研究其他场景下如何利用粘性标签进行隐私标签的嵌入, 并将本文提出的模型框架与现有的社交平台进行对接。

参考文献:

- [1] TIWARI B, KUMAR A. Role-based access control through on-demand classification of electronic health record[J]. International Journal of Electronic Healthcare, 2015, 8(1): 9.
- [2] GATES C E. Access control requirements for Web 2.0 security and privacy[C]//Proceedings of Workshop on Web 2.0 Security and Privacy. 2007: 249-256.

- [3] 姚瑞欣, 李晖, 曹进. 社交网络中的隐私保护研究综述[J]. 网络与信息安全学报, 2016, 2(4): 33-43.
YAO R X, LI H, CAO J. Overview of privacy preserving in social network[J]. Chinese Journal of Network and Information Security, 2016, 2(4): 33-43.
- [4] FONG P W L. Relationship-based access control: protection model and policy language[C]//ACM Conference on Data & Application Security & Privacy. 2011: 191-202.
- [5] RIZVI S Z R, FONG P W L, CRAMPTON J, et al. Relationship-based access control for an open-source medical records system[C]//The 20th ACM Symposium. 2015: 113-124.
- [6] GUO L, ZHANG C, FANG Y. A Trust-based privacy-preserving friend recommendation scheme for online social networks[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(4): 413-427.
- [7] CHENG Y, PARK J, SANDHU R. A user-to-user relationship-based access control model for online social networks[J]. IEEE Transactions on Dependable & Secure Computing, 2017, 13(4): 1-1.
- [8] CHENG Y, PARK J, SANDHU R. Attribute-aware relationship-based access control for online social networks[M]//Data and Applications Security and Privacy XXVIII. Springer Berlin Heidelberg, 2014: 292-306.
- [9] 李风华, 孙哲, 牛犇, 等. 跨社交网络的隐私图片分享框架[J]. 通信学报, 2019, 40(7): 1-13.
LI F H, SUN Z, NIU B, et al. Privacy-preserving photo sharing framework cross different social network[J]. Journal on Communications, 2019, 40(7): 1-13.
- [10] ANSHELEVICH E, BHARDWAJ O, USHER M. Friend of my friend: network formation with two-hop benefit[J]. Theory of Computing Systems, 2015, 57(3): 711-752.
- [11] 陈天柱, 郭云川, 牛犇, 等. 面向社交网络的访问控制模型和策略研究进展[J]. 网络与信息安全学报, 2016, 2(8): 1-9.
CHEN T Z, GUO Y C, NIU B, et al. Research progress of access control model and policy in online social networks[J]. Chinese Journal of Network and Information Security, 2016, 2(8): 1-9.
- [12] 唐文, 陈钟, 段云所. 公钥密码技术[J]. 网络安全技术与应用, 2001: 61-64.
TANG W, CHEN Z, DUAN Y S. Public key cryptography[J]. Network Security Technology and Application, 2001: 61-64.
- [13] 李风华, 孙哲, 吕梦凡, 等. 社交照片隐私保护机制研究进展[J]. 信息安全学报, 2018(2): 41-61.
LI F H, SUN Z, LYU M F, et al. Research progress of photo privacy-preserving mechanisms in online social network[J]. Journal of Cyber Security, 2018(2): 41-61.
- [14] KARJOTH G U, SCHUNTER M, WAIDNER M. Platform for enterprise privacy practices: Privacy-enabled management of customer data[C]//International Conference on Privacy Enhancing Technologies. 2002: 69-84.
- [15] BAKER E. EXIF Custom: Automatic image metadata extraction for Scratchpads and Drupal[J]. Biodiversity Data Journal, 2013, 1(1): e973.
- [16] 杨晓锋. 数码图像文件格式标准 Exif 解读[J]. 照相机, 2006(4): 69-71.
YANG X F. Interpretation of digital image file format standard Exif[J]. Camera, 2006(4): 69-71.

[作者简介]



谢绒娜(1976-), 女, 山西永济人, 北京电子科技学院副教授, 主要研究方向为网络与系统安全、访问控制、密码工程。



范晓楠(1997-), 女, 河北邢台人, 北京电子科技学院硕士生, 主要研究方向为信息安全、访问控制。



袁琳(1994-), 女, 安徽淮北人, 北京电子科技学院硕士生, 主要研究方向为信息安全、访问控制。



郭子晨(1996-), 男, 安徽宿州人, 北京电子科技学院硕士生, 主要研究方向为信息安全。



朱家玉(1996-), 女, 黑龙江大兴安岭人, 北京电子科技学院硕士生, 主要研究方向为信息安全、数据溯源。



史国振(1968-), 男, 河南济源人, 北京电子科技学院教授、博士生导师, 主要研究方向为人密码信息安全、信息论与编码理论。