doi:10.3969/j.issn.1001-2400.2014.06.030

面向多媒体社交网络的访问控制模型

陈庆丽，张志勇，向 菲，王 剑
(河南科技大学 信息工程学院，河南 洛阳 471023)

摘要：传统访问控制模型无法满足新兴的多媒体社交网络场景下的用户数量大、动态交互和内容共享等特点.为此，提出了一种基于用户主要社交关系属性，如用户类型、紧密度、内容分享深度和信任度等，面向多媒体社交网络的访问控制模型.通过自定义安全规则及其安全策略冲突消解，有效地解决了数字媒体访问使用和分享传播中的安全问题，适用于多媒体数字版权保护应用的实际需求.

关键词：多媒体社交网络；访问控制；安全规则；策略冲突
中图分类号：TP309 **文献标识码**：A **文章编号**：1001-2400(2014)06-0181-07

Research on the access control model for multimedia social networks

CHEN Qingli, ZHANG Zhiyong, XIANG Fei, WANG Jian
(Inf. Eng. Coll., Henan Univ. of Sci. & Technol., Luoyang 471023, China)

Abstract: Traditional access control models are not suitable for an emerging scenario of Multimedia Social Networks (MSNs), in which there are a large number of users, dynamic interaction and content sharing. The paper proposes an access control model for MSNs, based on users' major social relationships, such as relationship type, compactness, content sharing depth and trust. By the self-defined security rules and their security policies conflict elimination, the model effectively solves the security problem of access control and sharing dissemination on digital media, and it would apply to digital right management applications.

Key Words: multimedia social networks; access control; security rules; policy conflict

多媒体社交网络(Multimedia Social Networks，MSNs)，例如 YouTube、SongTaste 等，作为一种最方便地在线分享图像、视频和音频等多媒体内容的方式出现，使得人与人之间的交流与信息传播更加方便、快捷，但同时也存在着大量的如隐私泄露[1]、版权纠纷等安全问题，给互联网信息的安全传播带来了严重危害.针对这些安全问题，访问控制机制提供了一种可以在 MSNs 中有选择地分享多媒体内容的方法.访问控制机制决定哪些用户能够访问何种资源以及如何使用这些资源.

现有的多媒体社交网络下的访问控制主要有以下两类：基于关系的访问控制以及基于信任的访问控制.基于关系的访问控制更突出用户间关系对内容访问的重要性.文献[2] 提出了一种基于策略的访问控制模型，有助于保护用户在社交网络环境中的潜在威胁.文献[3]提出了一种以用户行为为中心的访问控制框架，确定了 4 个核心控制行为：属性、策略、关系和会话.文献[4]提出了一种针对物联网感知层的基于属性的访问控制机制，实现了灵活的细粒度访问控制和匿名的数据访问.基于信任的访问控制更能适应社交网络动态环境，确保数字内容的安全及用户隐私.文献[5]采用了一种多级的安全方法，信任是惟一的用于决定用户和资源安全级别的参数.文献[6]提出了一种基于二度“朋友”关系的分布式身份认证管理系统，实现了访问权

收稿日期：2013-08-25 **网络出版时间**：2014-04-04
基金项目：国家自然科学基金资助项目(61370220，61003234)；河南省科技创新人才计划杰出青年基金资助项目(134100510006)；河南省教育厅科学技术研究重点项目基础研究计划资助项目(13A520240，14A520048)
作者简介：陈庆丽(1988－)，女，河南科技大学硕士研究生，E-mail：chenqingli88@126.com.
通信作者：张志勇(1975－)，男，教授，博士，E-mail：xidianzzy@126.com.
网络出版地址：http://www.cnki.net/kcms/doi/10.3969/j.issn.1001-2400.2014.06.030.html

利和信任授权管理. 文献[7]提出了一种和信任相关的管理架构,包含了支持隐私防护的访问控制策略和机制. 执行了对包含可证明信息的数据的访问策略,提高了对高复杂性隐私相关策略的全支持. 针对 MSNs 下的访问控制, 文献[8]提出了一种个人数据访问控制模型,允许用户通过历史交互行为度量用户间信任,并依据跳数判断用户是否可以访问数据. 文献[9]提出了一种增强的基于角色的访问控制模型,使用了 Petri 网和模型检测技术.

笔者在深入分析多媒体社交网络中多媒体数字内容传播特性的基础上,提出了一种面向多媒体社交网络的访问控制模型 MSNAC(An Access Control Model for Multimedia Social Networks). 在本方案中,当用户申请访问内容提供者发布的多媒体数字内容时,平台基于关系类型、深度、紧密度、信任度 4 个访问控制参数,对用户进行评估,并根据评估结果拒绝或者接受用户访问多媒体数字内容.

1 MSNAC 的构建及形式化描述

1.1 MSNAC 的构建

用户之间的访问控制,即用户访问另一个用户的内容信息,访问的主体是用户,客体是多媒体数字内容. 本方案描述的是多媒体社交网络中的用户对多媒体数字内容的访问控制问题.

在本方案中,内容请求者(Requester,R)请求访问内容提供者(Provider,P)的多媒体数字内容(MultiMedia Digital Content,MMDC)时,平台基于关系类型、深度、紧密度、信任度 4 个访问控制参数,对用户进行评估,并根据评估结果接受或者拒绝用户访问多媒体数字内容. 模型中,多媒体数字内容可以被划分为多个离散的内容项,平台可以根据内容请求者的属性,对用户的访问实行多重离散的访问控制. 图 1 描述了 MSNAC.

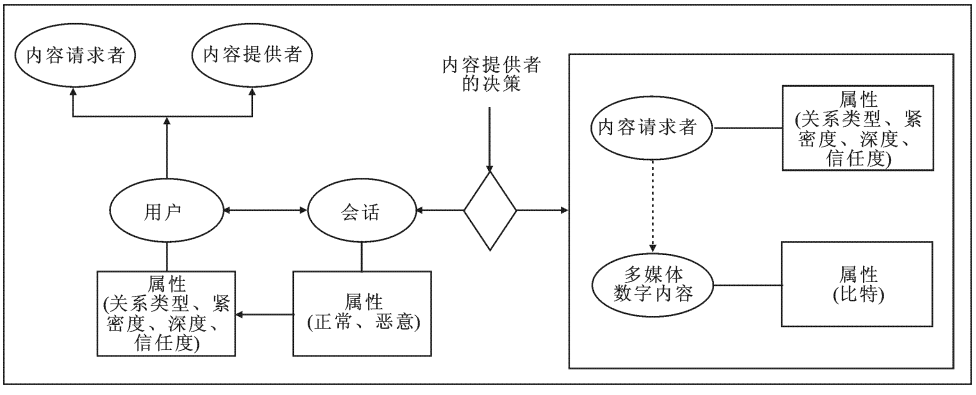

图 1 MSNAC

1.2 MSNAC 形式化定义

在 MSNAC 中,定义了会话,以及用户的属性:关系类型、深度、紧密度和信任度 6 个术语:

定义 1 会话(Session, S):R 向 P 请求 MMDC,P 根据 R 的属性有选择地响应 R,当 R 从 P 接收到所请求的 MMDC 时,记作一次会话.

会话可以分为恶意会话和正常会话两种,R 得到所需的、安全的数字内容或者权利,为正常会话,反之为恶意会话.

定义 2 关系类型(Relationship Type,RelT):内容提供者和内容请求者之间关系的类型.

对于内容提供者而言,每个 R 与 P 之间都有确定的关系类型. RelT 取值可以有多种,如“朋友”、“家人”等类似的社会关系类型. R 与 P 之间的关系类型可以有多种,例如,Alice 与 Bob 之间是家人关系,同时也是朋友关系.

定义 3 群组(Group, G):社交网络中的某些节点由于特定原因各自形成自己的小群体,它属于整个网络关系的一部分.

群组根据用户之间的关系类型分类,群组与用户的关系类型一一对应.

定义 4　深度(Depth,Dep):每个内容请求者之间以及内容请求者和内容提供者之间关联的最小跳数,即最短路径.

深度的计算方法采用 Dijkstra 算法,其值 Dep=1,2,…,n.

定义 5　紧密度(Compactness, C):在一定时间周期内,内容请求者和内容提供者之间信息交互的强度或频繁程度.

两者之间的信息交互强度越大、越频繁,其紧密度越高,C 值越大.C 的取值为正整数.内容提供者可以自定义交互次数基数.

定义 6　信任度(Trust, T):在一定时间周期内,信任评估者对受评估者的信任程度,具有动态特征,是由用户之间数字内容分享的历史行为信息决定的.

在多媒体社交网络环境下,P 与 R 间的分享会话中,R 得到所需的、安全的数字内容,为正常会话,反之为恶意会话.P 正常会话次数越多,其信任度越高,恶意会话次数越多,其信任度越低.信任度的变化范围是 $[0,1]$[10].

MMDC 可信反馈 R_c.用户访问 MMDC 后,用户可以根据所访问 MMDC 的安全可信程度对此次访问进行反馈,$R_c \in \{0,1\}$.其中 1 代表访问的 MMDC 是安全的,与内容提供者对 MMDC 的声明相符;0 代表访问的 MMDC 不可信、不安全.

时间衰减函数.根据信任度 T 的动态性和随时间的衰减性,信任关系强度随时间不断变化,最近的访问行为更能反映用户现在的信任程度.越久远的内容访问对当前信任评估的影响就越小,即其可信反馈在信任评估中所占的权重就越小,因此,定义时间衰减函数 $\omega(t)$ 为

$$\omega(t)=\left|(t_{\text{present}}-t_{\text{share}})/\delta\right| \quad , \tag{1}$$

其中,t_{present} 表示当前时间,t_{share} 表示分享所处的分享周期,δ 为信任衰减周期,代表信任关系每隔 δ 个分享周期衰减一次,$\delta \geqslant 1$.用户可以根据具体分享场景定义 δ 的大小,δ 越大,信任关系随分享周期衰减越慢,δ 越小,信任值随分享周期衰减越快.

设 P 和 R 的总分享周期为 N_t,得到 P,R 之间的直接信任度为

$$T=\frac{1}{N_t}\sum_{i=1}^{N_t}\frac{R_{c_i}(t)}{\omega_i(t)} \quad . \tag{2}$$

2　MSNAC 访问控制规则

MSNAC 中给出了内容请求者的 4 个基本属性,内容提供者可根据个人爱好或个性化需求定义其他属性;用户群组 G 可以看做用户形式上的静态分组,而用户的属性如深度、紧密度和信任度是动态变化的.粒度是对用户在逻辑上的动态分组.不同的属性通过“或门”、“与门”的操作刻画出不同的粒度.

2.1　访问控制模型形式化描述

访问权限是离散的访问控制参数,可以用访问权限向量 $\boldsymbol{L}$ 表示,$\boldsymbol{L}_P=\{l_1,l_2,\cdots,l_M\}$,$M$ 是访问权限的数量,即内容提供者对用户粒度的要求,每个内容提供者可以根据其需求自定义权限向量的变化范围.用户的属性可以用二进制向量 $\boldsymbol{A}$ 表示,$\boldsymbol{A}=\{A_1,A_2,\cdots,A_M\}$,属性向量中的每个属性与访问权限向量中各自的访问权限相对应.当用户的属性向量中的每个属性都符合访问权限向量中各自的访问权限时,用户可以访问多媒体数字内容 MMDC,即 $A_j \in l_j$,$\forall j \leqslant M$,可以访问 MMDC.

用户属性与权限向量的逻辑操作结果值用 B 表示,基本的变化范围包含 A_j 和 B_j 给出的二进制向量,B_j 表示第 j 个用户属性与访问权限第 j 个元素之间的逻辑运算结果值,其值为 1 或者 0.用户的 M 个访问权限之间可以进行 AND 操作,$B=B_1 \wedge B_2 \wedge \cdots \wedge B_M$,$B$ 获得最终值.当 B 为 1 时,接受此次访问请求,否则,拒绝此次访问.

用户属性与访问权限之间的对应关系分为两类:

(1) 如果访问权限对用户属性没有约束,则 B_j 为 1.

(2) 如果访问权限对用户属性有约束,则 $A_j \in l_j$ 时,B_j 为 1,否则 B_j 为 0.

本方案中,每一个访问权限都是一个单一的范围,但是在目前的多媒体社交网络中,访问权限大多有多个离散的范围. 例如一个用户可能需要访问一个内容的不同、不连续的部分. 因此,为了满足这一需求,笔者并未直接使用常规的模型,而是提出了一种具有多重离散范围的面向多媒体社交网络的访问控制模型.

2.2 多重离散范围的访问控制模型

在二进制向量中的每一个比特都与一个特定的内容一致. 如内容提供者的一个 MMDC 中有 N 个内容项,二进制向量的长度就是 N bit,内容项的比特划分可以由用户自定义. 例如,一段视频 V 可以被分为 N 个片段,这样内容请求者申请访问 V 时,可以不连续、离散地访问 V. 基本的变化范围包含 A_j 和由 B_j 给定的二进制向量. 如果它满足所有的 M 个访问内容的权限条件,即所有的权限中的第 n 个比特的 M 个二进制向量值都为 1,就可以访问这个内容. 所有权限值间进行 AND 操作,结果值为 B 的值.

2.3 MSNAC 基本约束规则

约束规则是 MMDC 的使用与分享传播时对用户所有属性的要求,保证了只有满足约束规则的用户访问 MMDC,有效保证了 MMDC 的安全性. 定义用户(包括 R,P)集合 U,多媒体数字内容集合 MMDC,群组集合 G,关系深度集合 Dep,关系深度常量 Dep_0,紧密程度集合 C,紧密程度常量 C_0,信任度集合 T,信任度常量 T_0,MMDC 的分类集合 O. $s(u \in U)$ 为内容请求者与内容提供者间的会话集合.

定义谓词 exec(u,s):用户 u 能够执行会话 s,谓词 exec(u,d),用户 u 可以访问 MMDC.

规则 1 如果一个用户没有注册多媒体社交网络,则无权开始一次会话.

$$\forall s(s \in S)(\mathrm{exec}(u,s)) \Rightarrow u \in U \quad .$$

规则 2 内容请求者不属于特定的群组,则无权访问多媒体数字内容.

$$\forall u,g(u \in U, g \in G)(\mathrm{exec}(u,d)) \Rightarrow \exists g(g \in G) \quad .$$

规则 3 用户和内容提供者不具备特定的关系深度,则无权访问多媒体数字内容.

$$\forall u,\mathrm{Dep}(u \in U, \mathrm{dep} \in \mathrm{Dep})(\mathrm{exec}(u,d)) \Rightarrow \exists \mathrm{dep}(\mathrm{dep} \leqslant \mathrm{Dep}_0) \quad .$$

规则 4 内容请求者和内容提供者不具备特定的紧密度,则无权访问多媒体数字内容.

$$\forall u,C(u \in U, c \in C)(\mathrm{exec}(u,d)) \Rightarrow \exists c(c \geqslant C_0) \quad .$$

规则 5 内容请求者和内容提供者不具备特定的信任度,则无权访问多媒体数字内容.

$$\forall u,T(u \in U, t \in T)(\mathrm{exec}(u,d)) \Rightarrow \exists t(t \geqslant T_0) \quad .$$

2.4 MSNAC 规则间的约束

约束 1 同一规则对于属于多个群组的同一用户,规则间通过逻辑运算("与"或者"或")避免相互冲突. 内容提供者对于 MMDC 的访问要求严格,执行规则间"与"操作;否则,执行规则间"或"操作.

(1) P 对于 MMDC 的访问要求严格:

$$\forall u,g\left(u \in U, g \in G_i, g \in G_j\right)(\mathrm{exec}(u,d)) \Rightarrow \exists g(g \in G_i \wedge g \in G_j) \quad .$$

(2) P 对于 MMDC 的访问要求松弛:

$$\forall u,g\left(u \in U, g \in G_i, g \in G_j\right)(\mathrm{exec}(u,d)) \Rightarrow \exists g(g \in G_i \vee g \in G_j) \quad .$$

约束 2 同一规则对于属于多个类别的同一 MMDC,规则间通过逻辑运算("与"或者"或")避免相互冲突. 内容提供者对于 MMDC 的访问要求严格,执行规则间"与"操作;否则,执行规则间"或"操作.

(1) P 对于 MMDC 的访问要求严格:

$$\forall u,o\left(u \in U, o \in O_i, o \in O_j\right)(\mathrm{exec}(u,d)) \Rightarrow \exists o(o \in O_i \wedge o \in O_j) \quad .$$

(2) P 对于 MMDC 的访问要求松弛:

$$\forall u,o\left(u \in U, o \in O_i, o \in O_j\right)(\mathrm{exec}(u,d)) \Rightarrow \exists o(o \in O_i \vee o \in O_j) \quad .$$

约束 3 转发的 MMDC 必须满足内容原始拥有者的访问控制需求.

3 应用实例与安全性分析

本模型的原型系统(http://www.sigdrm.org/drmvideo/)实现了多媒体社交网络下的访问控制,用户

可以动态改变其策略,细粒度地访问多媒体数字内容,有效地解决了数字媒体访问使用和分享传播中的安全问题,适用于多媒体数字版权保护应用的实际需求.

3.1　安全策略应用实例

在一个多媒体社交网络中,存在 5 个用户 $R_i(i=1,2,\cdots,5)$,用户 R_1 拥有多媒体数字内容 MMDC,R_3 拥有多媒体数字内容 MMDC′,用户 R_2 拥有转发的 MMDC,如图 2 所示.

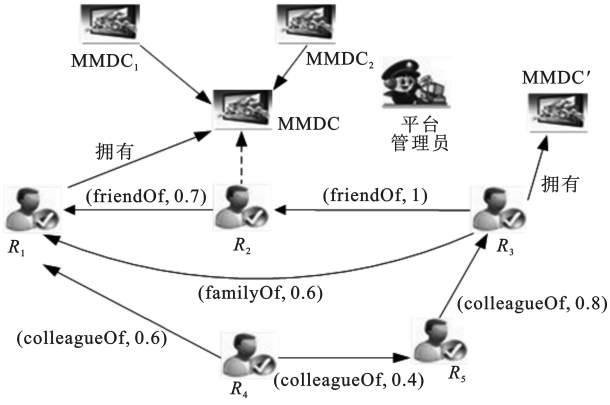

图 2　MSNAC 应用示例

MMDC 是一段视频,用户 R_1 指定其 MMDC 对于家人的权限向量 $\boldsymbol{L}=\{$家人,3,6,0.5$\}$,对于朋友的权限向量 $\boldsymbol{L}=\{$朋友,1,8,0.7$\}$. 假设用户 R_3 向用户 R_1 请求访问 MMDC,R_1 根据 MSNAC 验证 R_3 的属性,R_3 相对于 R_1 的属性向量 $\boldsymbol{A}_1=\{[$家人,朋友$]$,1,10,0.6$\}$. 当用户 R_1 对 MMDC 的访问要求严格时,根据 MSNAC 的规则约束,$B=1\wedge 1\wedge 1\wedge 0=0$,用户 R_1 拒绝 R_3 访问 MMDC;用户 R_1 对 MMDC 访问要求松弛时,$B=1\wedge 1\wedge 1\wedge 1=1$,允许 R_3 访问 MMDC. MMDC′是一首歌,它既属于乡村歌曲,又属于经典老歌. 用户 R_3 指定乡村歌曲类的权限向量 $\boldsymbol{L}=\{$同事,2,8,0.6$\}$,经典老歌类的权限向量 $\boldsymbol{L}=\{$同事,2,20,0.8$\}$. 假设用户 R_5 向用户 R_3 申请访问 MMDC′,R_3 根据 MSNAC 验证 R_5 的属性,R_5 相对于 R_3 的属性向量 $\boldsymbol{A}_2=\{$同事,1,12,0.8$\}$. 当用户 R_3 对 MMDC′的访问要求严格时,根据 MSNAC 的规则约束,$B=1\wedge 1\wedge 0\wedge 1=0$,用户 R_3 拒绝 R_5 访问 MMDC′;用户 R_3 对 MMDC′访问要求松弛时,$B=1\wedge 1\wedge 1\wedge 1=1$,允许 R_5 访问 MMDC′. MMDC 对于 R_2 是转发的内容,R_2 修改了 MMDC 对于内容请求者的属性要求,其权限向量 $\boldsymbol{L}=\{$朋友,2,4,0.5$\}$. 如果用户 R_3 向用户 R_2 请求访问 MMDC,R_3 相对于 R_2 的权限向量 $\boldsymbol{A}=\{$朋友,1,6,1$\}$,根据 MSNAC 中的规则约束 3,$B=1\wedge 1\wedge 0\wedge 0=0$,用户 R_3 被拒绝访问 MMDC.

R_1 指定其 MMDC 对于同事的权限向量为 $\boldsymbol{L}=\{$同事,1,20,0.7$\}$,内容请求者 R_4 的属性向量 $\boldsymbol{A}=\{$同事,1,20,0.6$\}$,$B=1\wedge 1\wedge 1\wedge 0=0$,$R_4$ 被拒绝访问 MMDC. 将 MMDC 分成两段:MMDC_1 和 MMDC_2,每一段对于 R 的权限要求不同,MMDC_1 对应的权限向量 $\boldsymbol{L}_1=\{$同事,1,20,0.7$\}$,MMDC_2 对应的权限向量 $\boldsymbol{L}_2=\{$同事,1,20,0.5$\}$. $B_1=11$,$B_2=11$,$B_3=11$,而 B_4 只满足 $\boldsymbol{L}_1$,则 $B_4=01$,$B=11\wedge 11\wedge 11\wedge 01=01$. 只有 MMDC_2 的比特位 1,因此 R_2 只能访问 MMDC_2.

3.2　功能与安全性分析

动态性:用户的属性如深度、紧密度和信任度是动态变化的,因此,本方案可以实现策略的动态变化.

访问粒度:多媒体数字内容被分为离散的数据项,每一个访问权利对应一个数据项,用户满足相应的访问权利时,可以访问数字内容. 实现了用户对多媒体数字内容的细粒度访问.

属性认证:内容提供者不需要主动认证用户的属性,而只需要检验用户属性是否满足门限条件. 用户的属性认证由系统完成,只有拥有合法属性的用户才可以访问多媒体数字内容.

策略冲突:同一规则对于属于不同分组的同一主体/客体,在主体请求访问客体时,出现策略冲突问题. 本方案提出了规则间的约束,有效避免了策略冲突问题.

笔者将提出的 MSNAC 从功能性与安全机制方面与几种典型的访问控制策略进行了对比分析,如表 1 所示.

现有的社交网络下的访问控制模型是静态、粗粒度、缺少主体社会属性考量、无法消解安全策略/规则的冲突的模型,而 MSNAC 综合考虑了现存模型的缺陷,构建了一个动态、细粒度、主体社会属性全面考量、消除了安全策略规则间冲突的访问控制模型,有效地保证了数字内容的安全分享和传播.

4　结 束 语

多媒体社交网络正处于普及的浪潮中,其安全问题日益凸显,得到了广泛的关注. MSNs 中存在大量并

表 1 几种典型的访问控制策略对比

功能性与安全机制	访问控制机制	访问粒度	信任度计算	关系	转发资源安全设置	策略冲突	系统开销	适合场景
Tencent 空间	基于分组、DAC	结合分组、DAC	无	直接、间接	否	否	适中	社交网络
UACF[3]	分离个人用户和资源策略	用户行为	行为	直接、间接	否	否	较大	在线社交网络
基于属性的访问控制机制[4]	属性证书	属性	无	直接	否	否	较小	物联网
TBAF[5]	关系、信任、目的和义务	属性	行为	直接、间接	否	否	适中	社交网络
TBAC[10]	个人数据	保护区间	行为	直接、间接	是	否	较小	社交网络
有效访问控制机制[11]	二进制向量转换	二进制向量转换	行为	直接、间接	否	否	较小	多媒体社交网络
RBAC[12]	证书	规则	证书链	直接、间接	否	否	较大	社交网络
MSNAC	关系类型、紧密度、信任度、深度	分组、属性	历史行为	直接、间接	是	否	较小	多媒体社交网络

发的数据访问,需要合理的访问控制机制来管理用户的数据访问权限.传统的粗粒度访问控制在 MSNs 中有很多局限,无法满足其安全需求.本方案综合考虑了访问控制中用户的属性,将用户和 MMDC 进行了分组,既保证了用户的隐私安全,满足了对 MMDC 的细粒度访问控制,对 MMDC 的分类及用户的分组处理,又减少了系统开销.提出的 MSNAC 考虑了策略冲突问题,策略中,约束间通过"与"或者"或"逻辑运算,避免了策略冲突问题. 这是目前社交网络访问控制模型中所未实现的.进一步的研究工作可以进行策略的博弈,以选择合理的访问控制策略,最大限度地避免拒绝正常用户访问 MMDC 及接受恶意用户访问 MMDC.

参考文献:

[1] 张志勇, 裴庆祺, 杨林, 等. 支持验证代理方的远程证明模型及其安全协议[J]. 西安电子科技大学学报, 2009, 36(1): 58-63.
Zhang Zhiyong, Pei Qingqi, Yang Lin, et al. Attestation Proxy Party-supported Remote Attestation Model and Its Secure Protocol [J]. Journal of Xidian University, 2009, 36(1): 58-63.

[2] Kim K, Hong S, Kim J Y. A Study on Policy-based Access Control Model in SNS[J]. International Journal of Multimedia and Ubiquitous Engineering, 2012, 7(3): 143-150.

[3] Park J, Sandhu R, Cheng Y. A User-Activity-Centric Framework for Access Control in Online Social Networks[J]. IEEE Internet Computing, 2011, 15(5): 62-65.

[4] 任方, 马建峰, 郝选文. 物联网感知层一种基于属性的访问控制机制[J]. 西安电子科技大学学报, 2012, 39(2): 66-72.
Ren Fang, Ma Jianfeng, Hao Xuanwen. Attribute-based Access Control Scheme for the Perceptive Layer of the Internet of Things[J]. Journal of Xidian University, 2012, 39(2): 66-72.

[5] Ali B, Villegas W, Maheswaran M. A Trust Based Approach for Protecting User Data in Social Networks[C]// Proceedings of the 2007 Conference of the Center for Advanced Studies on Collaborative Research. New York: ACM, 2007: 288-293.

[6] Kruk S R, Grzonkowski S, Gzella A, et al. D-FOAF: Distributed Identity Management with Access Rights Delegation [M]. Heidelberg: Springer, 2006: 140-154.

[7] Wang H, Sun L. Trust-involved Access Control in Collaborative Open Social Networks[C]//Proceedings of 4th International Conference on Network and System Security. Piscataway: IEEE, 2010: 239-246.

[8] Villegas W. A Trust-based Access Control Scheme for Social Networks[D]. Montreal: McGill University , 2008.

[9] Ding J, Mo L. Enforcement of Role Based Access Control in Social Network Environments[C]//IEEE Sixth International Conference on Software Security and Reliability Companion. Piscataway: IEEE, 2012: 92-101.

[10] Zhang ZY, Wang KL. A Trust Model for Multimedia Social Networks[J]. Social Networks Analysis and Mining

(Springer), 2013, 3(4): 969-979.

[11] Sachan A, Emmanuel S, Kankanhalli M S. An Efficient Access Control Method for Multimedia Social Networks[C]//Proceedings of Second ACM SIGMM Workshop on Social Media. New York: ACM, 2010: 33-38.

[12] Carminati B, Ferrari E, Perego A. Rule-based Access Control for Social Networks[C]//Lectures Notes in Computer Science: 4278. Heidelberg: Springer Verlag, 2006: 1734-1744.

(编辑：李恩科)

(上接第 136 页)

[3] Podlipnig S, Böszörmenyi L. A Survey of Web Cache Replacement Strategies [J]. ACM Computing Surveys, 2003, 35(4): 374-398.

[4] 唐丽均, 李云, 柴毅, 等. 一种结合传染路由的缓存调度算法 [J]. 西安电子科技大学学报, 2012, 39(1): 141-145.
Tang Lijun, Li Yun, Chai Yi, et al. Buffer Schedule Algorithm Combined with Epidemic Routing [J]. Journal of Xidian University, 2012, 39(1): 141-145.

[5] Chai W K, He D, Psaras I, et al. Cache "Less for More" in Information-centric Networks (Extended Version) [J]. Computer Communications, 2013, 36(7): 758-770.

[6] Cho K, Lee M, Park K, et al. WAVE: Popularity-based and Collaborative In-network Caching for Content-oriented Networks [C]//Conference on Computer Communications Workshops. Piscataway: IEEE, 2012: 316-321.

[7] Psaras I, Chai W K, Pavlou G. Probabilistic In-network Caching for Information-centric Networks [C]//Proceedings of the Second Edition of the ICN Workshop on Information-centric Networking. New York: ACM, 2012: 55-60.

[8] Zhang G, Li Y, Lin T. Caching in Information Centric Networking: a Survey [J]. Computer Networks, 2013, 57(16): 3128-3141.

[9] Li J, Liu B, Wu H. Energy-efficient In-network Caching for Content-centric Networking [J]. IEEE Communications Letters, 2013, 17(4): 797-800.

[10] Carofiglio G, Gallo M, Muscariello L. On the Performance of Bandwidth and Storage Sharing in Information-centric Networks [J]. Computer Networks, 2013, 57(17): 3743-3758.

[11] Wang J M, Zhang J, Bensaou B. Intra-AS Cooperative Caching for Content-centric Networks [C]//Proceedings of the 3rd ACM SIGCOMM Workshop on Information-centric Networking. New York: ACM, 2013: 61-66.

[12] Adamic L A, Huberman B A. Zipf's Law and the Internet [J]. Glottometrics, 2002, 3(1): 143-150.

(编辑：郭　华)