基于RBAC的隐私访问控制研究

张学明 黄志球 孙 艺

(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要 基于角色的访问控制(Role-Based Access Control,RBAC)在Web服务隐私保护中可用于控制服务提供者对用户隐私数据的访问。针对RBAC运用于隐私场景中缺少相应的隐私属性而无法精确地描述隐私访问控制策略这一问题,提出了一种以RBAC为中心的隐私访问控制模型,给出了服务提供者信誉度分级方法。对不同信誉度等级的服务提供者分配不同的角色,以控制其对敏感隐私信息的访问。最后通过实例验证了该模型的有效性和可行性。

关键词 角色访问控制,隐私授权,信誉度,敏感度

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.038

Research on Privacy Access Control Based on RBAC

ZHANG Xue-ming HUANG Zhi-qiu SUN Yi

(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract RBAC can be used to control the service provider to access the privacy of users in Web service. In order to solve the problem that RBAC cannot precisely describe the privacy access control policy for the lack of privacy attributes when it is applied in the privacy scene, this paper put forward a privacy access control model focused on RBAC, and provided the ranking method of the credibility of the service provider. Service providers with different credibility ranks were assigned with different roles to control their access to the sensitive privacy information. This paper also verified the validity and feasibility of the model through a specific example.

Keywords Role-based access control, Privacy authorization, Credibility, Sensitivity

1 引言

随着互联网的不断发展,用户对于Web服务的依赖性越来越强,传统的Web服务模式虽然能够满足用户的服务需求,但是对于用户的隐私信息没有足够的保障。近年来,国内外很多学者致力于研究Web服务模式下用户隐私信息的保护问题。在Web服务中,用户在接受Web服务的同时需要向服务方提供必须的隐私信息,由于其开放和动态的特性,用户在提供个人隐私信息时无法得知自己的隐私信息将被如何使用。因此,很多信誉度低的服务提供者会通过非法获取用户的隐私信息来获益,这将给用户带来巨大的损害。如何有效地保护个人隐私问题成为关注的焦点。

为了保护用户的隐私信息,产业界已经提出了许多隐私保护的技术和标准。W3C组织提出的隐私偏好平台(Platform for Privacy Preferences,P3P)[1]提供了一个比较完整的框架来定义隐私策略,给出了一种标准的、机器可读的隐私策略定义语法,可以自动分析和清楚表现服务提供者的隐私策略。企业隐私授权语言(Enterprise Privacy Authorization Language,EPAL)[2]是一种形式化语言,被用来编写管理计算机系统中数据处理实践的企业隐私策略。其他的方法包括将隐私信息通过程序密封(如TRUSTe,ESRB,BBBOnline和CPAWebTrust)等。然而,当用户隐私数据被收集后,这些技术与方法无法提供系统的机制来指定和控制用户个人数据的处理方式。因为当用户提交隐私信息后,服务提供者在遵守发布的隐私策略下可以获取到用户的隐私信息,但是,服务提供者的实际操作可能会有意或者无意地违背发布在他们网站上的隐私策略,从而泄漏用户的隐私数据[3]。

为了保护用户的隐私信息,一种支持隐私需求能力的访问控制(Access Control,AC)模型被提出,用于帮助用户控制个人信息[4-6]。访问控制是通过某种途径显式地准许或限制访问能力及范围,从而限制用户对目标资源的访问,防止非法用户的侵入或合法用户的不慎操作所造成的破坏。常规的访问控制模型包括自主访问控制(Discretionary Access Control,DAC)、强制访问控制(Mandatory Access Control,MAC)和基于角色的访问控制(Role-Based Access Control,RBAC)[7]。自主访问控制允许资源的所有者自主地在系统中决定可存取其资源客体的主体,此模型灵活性很高,但安全级别相对较低;强制访问控制的主体权限和客体安全属性都是固定的,由管理员通过授权决定一个主体对某个客体能否进行访问。无论是DAC还是MAC,它们都是主体和访问权限直接发生关系,根据主体/客体的所属关系或主体/客体的安全级别来决定主体对客体的访问权,其优点是管理集中,但

到稿日期:2014-12-03 返修日期:2015-03-02 本文受国家自然科学基金(61272083)资助。

张学明(1990-),男,硕士生,主要研究方向为Web服务、Web隐私等,E-mail:xuemingzhang90@163.com;**黄志球**(1965-),男,博士,教授,主要研究方向为软件工程、Web服务、Web隐私等;**孙 艺**(1989-),女,硕士生,主要研究方向为Web服务、Web隐私等。

其实现工作量大，不便于管理，不适用于主体或客体经常更新的应用环境。RBAC是一种可扩展的访问控制模型，通过引入角色来对用户和权限进行解耦，简化了授权操作和安全管理，是目前公认的解决资源访问控制的有效访问方法。

RBAC模型是David Ferraiolo和Rick Kuhn合作在访问控制模型的基础上于1992年提出的，之后成为具有影响力的高级访问控制模型，在管理大型网络服务安全时表现了灵活性和经济性[8]。在RBAC中，在用户(User)和访问权限(Permission)之间引入角色(Role)的概念，用户与特定的一个或者多个角色相联系，角色与一个或者多个访问权限相联系，角色可以根据实际的工作需要生成或者取消。在隐私场景中，服务请求者提供隐私信息，服务提供者作为用户获取服务请求者的隐私信息提供服务。现有的大多数方法依赖于服务提供者的自觉性，即服务提供者能够主动执行服务的隐私策略要求，达到保护用户隐私信息的目的；然而通过RBAC可以有效地控制服务提供者对服务请求者敏感隐私信息的访问，该方法直接从根源上对服务提供者的隐私信息使用权限进行约束。

RBAC模型由于缺少隐私规则相应的属性，特别是目的绑定(如未经用户的允许，不可以将用于某个目的的用户信息用于其他的目的)、条件和义务，并非旨在加强隐私策略和满足隐私保护需求。尽管存在这一限制，但是现有的访问控制模型可以作为起点来控制用户的个人隐私信息。因为访问控制的安全策略和隐私策略通常都是控制访问相同的资源，并且都用于简化管理，所以它们并不会产生冲突[3,9]。

本文详细分析了用户隐私信息访问控制需求，提出了一种以RBAC为中心的隐私信息访问控制模型。首先给出访问控制策略，然后通过对隐私信息进行敏感度分级和对服务提供者进行信誉度分级，严格区分出隐私信息的重要程度。其次，将分级后的隐私信息通过角色访问控制模型分配给不同的角色，不同等级的服务通过不同的信誉等级获取角色，以达到控制隐私信息非法使用的目的。通过对隐私信息的访问控制，可以从根源上对服务提供者使用隐私信息的权限进行约束，即服务提供者需要具备良好的信誉并严格遵守保护用户隐私的策略要求，才可以获取用户的隐私信息。

本文第2节提出了基于角色的隐私访问控制模型；第3节提出了一种评估服务信誉度和隐私敏感度的方法；第4节描述了隐私访问控制的流程；第5节进行了案例分析；第6节是相关工作；最后总结全文。

2 基于角色的隐私访问控制模型(PRBAC-Model)

本文首先给出了基于角色的隐私访问控制模型，图1是模型的结构图。它主要包括一组实体集：*Subject*(*S*)，*Roles*(*R*)，*Objects*(*O*)，*Actions*(*A*)，*Purposes*(*Pu*)，*Obligations*(*Ob*)和*Conditions*(*C*)，定义2对这些实体集进行了描述。在PRBAC中，权限分配表示为隐私访问控制策略，定义1给出了隐私访问控制策略的定义，本文使用隐私访问控制策略规约服务在执行某个操作时能访问一组隐私的权限。这与传统的RBAC模型中的权限不同，在PRBAC中增加了可以用来表达隐私信息的条件、目的和义务。隐私访问控制模型主要的思想是通过*Conditions*控制服务提供者对用户隐私信息的访问，服务提供者获取到用户的隐私信息的前提是他必须获取到具有相应隐私信息访问权限的角色。

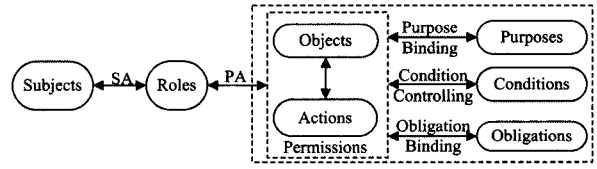

图1 隐私访问控制模型结构

在模型中，*Subject*代表服务主体，表示服务提供者，主体具有相应的属性值*subject. attribute*，如服务提供者的信誉度。*Role*代表服务中具有一定权力和责任的某种职权或者职称，将这些职能或者职称授予*Role*，如授予*Role*高级服务、普通服务等。模型中的*Role*一方面通过权限授权*PA*与一组服务用户关联，表示角色的访问权限规范；另一方面通过身份授权*SA*与一组服务提供者关联，表示角色的用户成员。*Object*代表服务请求者的隐私信息集，带有相应的属性值*object. attribute*，如隐私信息集的敏感度。*Action*是可执行的操作，一旦被调用，将会为服务提供者执行访问服务请求者隐私信息集的功能。*Purposes*表示服务提供者访问用户隐私信息的目的，如*service_release*等；*Conditions*表示服务提供者访问用户隐私信息的条件，如服务信誉度满足隐私敏感度；*Obligations*表示服务提供者获取用户隐私后需要满足相应的义务，如*Notify*(*ByEmail*)等。

在PRBAC中，基于角色的授权原理是，先确定角色对隐私访问的权限规范，*Permissions*被相应地分配给*Roles*，服务提供者通过被授予相应的角色来获取访问隐私信息的权限。PRBAC具有复杂的隐私权限分配结构，可以反映隐私规则的高度结构化的过程。因此除了基本的数据和操作之外，*Permission*可以准确地表述*Purposes*、授予权限所必需的*Conditions*、还有授予权限后所要承担的*Obligations*。举一个简单的例子，美国儿童在线隐私保护法(The Children's Online Privacy Protection Act，COPPA)中要求服务提供者访问儿童隐私信息时必须满足"获得父母同意的认证"，只有在满足这一条件的提前下，服务提供者才可以披露儿童的隐私敏感信息[3]。

定义1(隐私访问控制策略，Access Control Strategy)
一条隐私访问控制策略可以定义为$plcy=(s,r,(a,o),c,pu,ob)$，其中$s\in S$表示一个服务；$r\in R$表示一个角色；$a\in A$表示一个操作，它可以是隐私信息的接收操作；$o\in O$表示一个操作对象，它可以是用户的隐私信息；$c\in C$表示一个条件，条件用隐私权限矩阵表示(如图2所示)；$pu\in Pu$表示一个目的，如{*marketing*}表示一个进行销售的服务目的；$ob\in Ob$表示一个义务，如{*Notify*(*ByEmail*)}表示一个需要通过Email通知用户的义务。

为了易于表达和理解，一个隐私访问控制策略*plcy*可以表达为如下的形式：〈*subject*〉[WITH 〈*subject. attribute*〉]GET 〈*role*〉CAN 〈*action*〉ON 〈*object*〉[WITH 〈*object. attribute*〉]FOR 〈*purposes*〉WITH 〈*obligations*〉IF 〈*conditions*〉。

隐私访问控制规则可以通过严格的XML模式实现[10]。为了规则的清晰性和简明性，隐私访问控制规则都将通过上述的形式表达。举一个简单的例子，表1展示了一个访问控制策略的两个策略和描述，及控制服务对Alice和Bob隐私数据的访问。

表 1　隐私访问控制规则示例

	AC 策略	描述
AC_1	sp_1(WITH sp_1. credit) GET $role_1$ CAN read ON Alice_info WITH (Alice_info. sensitivity) FOR {marketing, service_release} WITH {Notify (ByEmail)} IF {sp_1. credit satisfy Alice_info. sensitivity}	当 sp_1 的信誉度满足访问的隐私数据集 Alice_info 的敏感度时，sp_1 获得 $role_1$ 授权访问 Alice_info 用于 marketing 和 service_release，当 sp_1 获得信息后必须完成使用 Email 通知 Alice 的义务。
AC_2	sp_2 WITH sp_2. credit GET $role_2$ CAN read ON Bob_info WITH Bob_info. sensitivity FOR service_release WITH {Notify(ByEmail)} IF{sp_2. credit satisfy Bob_info. sensitivity}	当 sp_2 的信誉度满足访问的隐私数据集 Bob_info 的敏感度时，sp_2 获得 $role_2$ 授权访问 Bob_info 用于 service_release，当 sp_2 获得信息后必须完成使用 Email 通知 Bob 的义务。

隐私访问控制策略中 *Conditions* 使用三角矩阵表示一组隐私权限，该矩阵称为隐私权限矩阵，如图 2 所示，其中矩阵的行坐标表示一组角色类型，而列坐标则表示一组隐私数据对象，隐私数据对象根据对象集的敏感度(Sensitivity)值依次变小的顺序排列，如 P_1 的敏感度值大于 P_2，P_2 的敏感度值大于 P_3，依次类推。矩阵中的元素值 0 表示 0 元素所对应的角色不可以访问相对应的隐私数据对象；矩阵中的元素值 1 表示 1 元素所对应的角色可以访问相对应的隐私数据对象。

	$Role_1$	$Role_2$	$Role_3$	…	$Role_n$
P_1	1	0	0	…	0
P_2	1	1	0	…	0
P_3	1	1	1	…	0
⋮	⋮	⋮	⋮		⋮
P_n	1	1	1	…	1

图 2　隐私权限矩阵

对访问权限的设置需要考虑服务的信誉度。本文使用敏感度差值计算方法，即通过将服务按照信誉度值的大小进行排列，使用相邻的两个信誉度值进行差值计算，当服务 i 与服务 j 的信誉度差值大于某个值 $\beta(\beta\geqslant 0$，β 称为调节因子，可以通过改变 β 的大小来严格控制服务被授予的角色的隐私访问权限)时，服务 i 和信誉度值在服务 i 之前的服务将被授予角色的隐私访问权限高于服务 j 和信誉度值在服务 j 之后的服务。例如，有 m 个服务($s_1,s_2,s_3,\cdots,s_m$)参与排列，计算 $s_1-s_2,s_2-s_3,\cdots,s_i-s_j,\cdots,s_{m-1}-s_m$，当 s_i-s_j 的差值大于 β 时，$s_1,s_2,\cdots,s_i$ 被授权 $Role_1$，信誉度值在 s_j 与下一次差值大于 β 的服务之间的服务被授权 $Role_2$，依次类推，最后所有服务都将被授予相应的角色，并且可以根据服务信誉度的情况，通过改变调节因子 β 来控制服务被授予的角色的隐私访问权限。

访问权限设置的原则是：高信誉度的服务可以访问敏感度高的隐私数据对象集，同时也可以访问敏感度低的隐私数据集；低信誉度的服务只可以访问敏感度低的隐私数据对象集，无法访问敏感度高的隐私数据集。如果服务迫切想要访问某一隐私数据对象集，但是信誉度无法满足要求，则需要通过访问主体与客体之间的隐私协商来解决(本文不对协商进行讨论)，具体可参考文献[11]。

根据隐私访问控制策略，定义一个服务的隐私访问控制模型。

定义 2(隐私访问控制模型)　一个服务的隐私访问控制模型定义为 $prbac=(S,R,A,O,C,Pu,Ob,PLCY,F_{cm})$，其中 S 表示一组有穷的服务主体集；R 表示一组有穷的角色集；A 表示一组有穷的操作集；O 表示一组有穷的对象集；C 表示一组有穷的条件集；Pu 表示一组有穷的目的集；Ob 表示一组有穷的义务集。$PLCY\subseteq S\times R\times C\times A\times O\times Pu\times\rho(Ob)$，表示隐私权限策略的集合，其中 $\rho(Ob)$ 表示 Ob 的幂集，对任意的 $(s,r,(a,o),c,pu,ob)\in PLCY$，规定服务 s 在执行操作 a 时能访问一组隐私的权限；$F_{cm}:(S_i,P_j)\rightarrow C$ 表示一个映射函数，用于获取服务 $S_i(0<i<n)$ 和隐私数据集 $P_j(0<j<n)$ 所构成的隐私权限矩阵。

3　服务信誉度与隐私信息敏感度分级

3.1　服务信誉度分级

定义 3(服务信誉度)　服务信誉度是服务质量(Quality of Service，QoS)的量化描述和所有服务用户在使用某个服务后给出的用户感知的概述，而这种概述一般是通过用户的反馈值来量化表达的。

对 Web 服务信誉度的评价过程中，既应该考虑服务自身的质量，也应该考虑用户的使用评价。服务提供者在提供服务过程中，在一定的时间内，其信誉度值会随着服务质量和用户的使用评价的改变而发生变化。本文假设服务在较短的时间内，其服务质量和用户的评价未发生改变(或改变不足以对服务的信誉度值产生影响)，计算的服务信誉度将不会发生改变。

Web 服务的 QoS 属性多种多样且度量单位各不相同，评价服务信誉度首先要对这些 QoS 进行规范化处理。根据规范化后的 QoS 值计算 QoS 综合值[12]。假设有 n 个服务 $S=\{s_1,s_2,s_3,\cdots,s_n\}$，每个服务有 m 个 QoS 属性 $Q=\{q_1,q_2,q_3,\cdots,q_m\}$，每个服务的 QoS 属性表示为 q_{ij}(i 表示某个服务，j 表示某个属性)，n 个服务的 m 个 QoS 属性可以表示为：

$$Q=\begin{pmatrix} q_{11} & q_{12} & q_{13} & \cdots & q_{1m} \\ q_{21} & q_{22} & q_{23} & \cdots & q_{2m} \\ q_{31} & q_{32} & q_{33} & \cdots & q_{3m} \\ \vdots & \vdots & \vdots & & \vdots \\ q_{n1} & q_{n2} & q_{n3} & \cdots & q_{nm} \end{pmatrix}$$

由于 QoS 属性中，有些属性的值越大，服务质量越低(负属性)，如延迟时间、增大花费等；有些属性的值越大，服务质量越高(正指标)，如可靠性、可用性等。因此需要对这些属性值进行规范化处理，引入一个向量 $T=\{t_1,t_2,t_3,\cdots,t_n\}$，其中，$t_i(0<i<m)$ 的取值为 -1 或 1，当 $t_i=1$ 时，表示属性值越大，服务质量越高；当 $t_i=-1$ 时，表示属性值越大，服务质量越低。Q 中每一个元素可以使用式(2)进行规范化：

$$q'_{ij}=\begin{cases}\dfrac{q_{ij}-q_{\min}}{q_{\max}-q_{\min}}*v_j, & q_{\max}-q_{\min}\neq 0\\ 1, & q_{\max}-q_{\min}=0\end{cases} \tag{2}$$

式中，$q_{\min}$ 和 $q_{\max}$ 分别表示矩阵某一列向量的最大值和最小值。

根据规范化后的 QoS 属性值计算 Web 服务的 QoS 综合值，计算公式如下：

$$QoS(s_i)=\frac{1}{m}\sum_{j=1}^{m}q'_{ij}+m \tag{3}$$

得出服务的 QoS 综合值并且用户对服务做出评价后，可

以结合这两个因素计算服务信誉度，公式如下：

$$SR(s_i)=w*QoS(s_i)+(1-w)*\frac{\sum_{j=1}^{j=n}R_j(s_i)}{n} \quad (4)$$

式中，$SR(s_i)$为服务 s_i 的信誉度，$QoS(s_i)$为服务 s_i 的 QoS 综合值，$R_j(s_i)$为用户 j 对服务 s_i 的评价值，取值范围为[0,1]。w 表示权值，取值范围为[0,1]。当 $w=1$ 时，表示评估服务信誉度时不考虑用户的评价。当 $w=0$ 时，表示评估服务信誉度时不考虑服务的客观服务质量。在实际应用中，管理人员可以根据具体的情况合理选择权值 w 的大小。

假设有如下 3 个 Web 服务，每个服务的 QoS 值如表 2 所列。

表 2　Web 服务 QoS 属性表

服务名	响应时间(ms)	可靠性	价格
Taobao	600	0.7	1.2
Box_Store	400	0.9	1.0
Meituan	500	0.8	2.0

本例中，只取响应时间、可靠性和价格 3 个属性进行计算。可以由这 3 个 Web 服务的 QoS 组成一个矩阵：

$$Q=\begin{bmatrix}q_{11} & q_{12} & q_{13}\\ q_{21} & q_{22} & q_{23}\\ q_{31} & q_{32} & q_{33}\end{bmatrix}=\begin{bmatrix}600 & 0.7 & 1.2\\ 400 & 0.9 & 1.0\\ 500 & 0.8 & 2.0\end{bmatrix} \quad (5)$$

矩阵 Q 的列依次表示服务响应时间、服务可靠性和服务价格。实际中，服务响应时间和服务价格的增加会对服务质量产生负影响性，服务可靠性的增加会对服务质量产生正影响性，因此向量 T 可用{−1,1,−1}表示。利用式(2)和式(3)可以计算出 3 个 Web 服务的 QoS 综合值依次为 2.60，3.33，2.67。

同时有 4 位用户对 3 个 Web 服务进行评价，对服务的评价值如表 3 所列。

表 3　Web 服务用户评价表

用户 \ 服务名	Taobao	Box_Store	Meituan
$user_1$	0.6	0.8	0.7
$user_2$	0.6	0.7	0.6
$user_3$	0.7	0.8	0.7
$user_4$	0.6	0.7	0.7

假设 w 的取值为 0.6，即 QoS 的比重高于用户的评价，最后利用式(4)可以计算出 3 个 Web 服务的信誉度值依次为 1.81，2.298，1.872，可以看出，服务 Box_Store 的信誉度是最高的。

3.2　隐私信息敏感度分级

定义 4(隐私信息敏感度)　敏感度是一个度量隐私信息敏感程度的指标。设 P 是一组有穷的隐私信息集，对任意一个隐私信息 $p\in P$，函数 $f_w(p)$用于获取它的敏感度，其中 $f_w(p)\in[0,1]$，0 表示不敏感，1 表示十分敏感，值越大则敏感程度越高[13]。

本文的隐私信息敏感度由用户来评价，我们在公共平台上建立评价机制，目前很多信誉良好的网站都可以提供评价机制，用户根据隐私信息被暴露后产生的危害程度进行敏感度评分。本文设用户 i 对隐私信息 j 的当前敏感度评分为 $r_{i,j}$，$r_{i,j}\in\{0,1,2,3,4,5,6,7,8,9\}$。若用户 i 认为隐私信息 j 造成的隐私危害比较大，则评分 $r_{i,j}$ 就比较低；反之当用户 i 认为隐私信息 j 造成的隐私危害比较小时，则评分 $r_{i,j}$ 就比较高。

评分以后，可以从上述网站收集到所需服务的评分，收集到的评分在 0 到 9 之间。一般我们定义的隐私信息敏感度属于[0,1]区间，因此需要将收集到的评分转换到[0,1]上，可使用式(6)进行转换：

$$td=tr*\frac{1}{9} \quad (6)$$

其中，tr 表示隐私信息的评分，td 表示隐私信息敏感度。

通过上述步骤，就可以获得隐私信息敏感度，且敏感度取值在 0 到 1 之间。

3.3　隐私信息集敏感度计算

定义 5(隐私信息集)　设 P_i 表示单个的隐私信息，隐私信息集是指由多个单个隐私信息组成的集合，可表示为$\{P_1,P_2,P_3,\cdots,P_n\}$。

定义 6(隐私相关度)　是指任意两个隐私项 P_i 和 P_j 相互关联对用户产生的影响程度的指标，可表示为 R_{ij}，其中$R_{ij}\in[0,1]$。两个隐私项关联对用户产生的影响越大，那么它们之间的相关度 R_{ij} 就越大；反之，R_{ij} 就越小。

在 Web 服务中，服务提供者收集的用户的信息都是一组隐私信息集，而不是单个的隐私信息。本文 3.2 节主要介绍了单个隐私信息的敏感度，用户单个的隐私信息并不会对用户个人造成伤害，例如，当服务提供者获取到用户的姓名时，对于服务提供者而言，获得用户的姓名并不能获取到任何对用户不利的信息。但是，当多个单个隐私信息组合成为隐私信息集时，隐私信息集会不同程度地对用户造成伤害，所以本文在单个隐私信息敏感度的基础上提出了隐私信息集敏感度的计算方法。本文首先同样通过用户评价的形式确定任意两个隐私信息之间的隐私相关度，然后通过式(7)计算出一组隐私信息集的敏感度。

$$F_p=\sum_{i=1}^{n}\sum_{j=1}^{n}R_{ij}*(p_i+p_j) \quad (7)$$

其中，F_p 表示$\{P_1,P_2,P_3,\cdots,P_n\}$所组成隐私信息集的敏感度，$R_{ij}$ 表示 P_i 和 P_j 的隐私相关度，p_i 和 p_j 表示 P_i 和 P_j 的隐私敏感度。例如，假设隐私信息 P_1={姓名}，P_2={电话号码}，P_3={地址}，P_4={银行卡号}的隐私敏感度值分别为 0.5，0.6，0.6，0.7，建立 P_1，P_2，P_3，P_4 之间的关系，如图 3 所示，R_{12}，R_{13}，R_{14}，R_{23}，R_{24}，R_{34} 表示任意组合的两个隐私项的隐私关联度。图 4 表示 P_1，P_2，P_3，P_4 中任意组合的两个隐私项的隐私关联度的值。

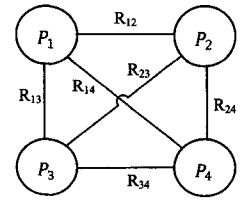

图 3　隐私项关系

P_1-P_2：$R_{12}=0.6$；

P_1-P_3：$R_{13}=0.5$；

P_1-P_4：$R_{14}=0.7$；

P_2-P_3：$R_{23}=0.5$；

P_2-P_4：$R_{24}=0.8$；

P_3-P_4：$R_{34}=0.6$。

图 4　任意两个隐私项的相关度

由于不同的服务对隐私集的需求不同，P_1，P_2，P_3，P_4 这

4 个隐私项可以任意组合；不同的组合的隐私集敏感度也是不同的，隐私集敏感度值越大表示在 Web 服务中隐私集越应当被保护。比如，在图中可以选择 P_2，P_3 作为一组隐私集；P_3，P_4 作为一组隐私集；P_1，P_2，P_3 作为一组隐私集；P_1，P_2，P_3，P_4 作为一组隐私集。通过式(7)计算出这几组隐私集的敏感度，如图 5 所示。

$F_{P_{(P_1,P_2)}}=0.66$　　$F_{P_{(P_1,P_3)}}=0.55$

$F_{P_{(P_1,P_4)}}=0.84$　　$F_{P_{(P_2,P_3)}}=0.60$

$F_{P_{(P_3,P_4)}}=0.78$　　$F_{P_{(P_2,P_4)}}=1.04$

$F_{P_{(P_1,P_2,P_3)}}=1.81$　　$F_{P_{(P_1,P_2,P_4)}}=2.54$

$F_{P_{(P_1,P_3,P_4)}}=2.71$　　$F_{P_{(P_2,P_3,P_4)}}=2.42$

$F_{P_{(P_1,P_2,P_3,P_4)}}=4.47$

图 5　隐私数据集敏感度

从图 5 中可以发现，在选择的几组隐私集中，$F_{(P_{P_1},P_2,P_3,P_4)}$ 的隐私集敏感度值是最大的，所以 P_1，P_2，P_3，P_4 与其他的隐私集相比具有更高的敏感度，更不容易被一般的服务提供者所获取。当隐私集敏感度处于相似情况下时，本文采用隐私数据最小暴露的原则，即当隐私信息集敏感度处于相似的情况下时，选取的最优隐私信息集一方面满足服务提供者提供服务的隐私需求，另一方面满足隐私信息的最小暴露原则。

4　隐私访问控制流程

隐私访问控制流程共包括 7 个功能组件：策略执行点(Policy Enforcement Point，PEP)，策略决策点(Policy Decision Point，PDP)，策略管理点(Policy Administration Point，PAP)，策略信息点(policy Information Point，PIP)，策略库(Policy Repository)，环境处理者(Context Handler)和信息管理者(Information Manager，IM)。其中策略库用于存储访问控制策略，PAP 对这些策略提供管理，如策略的设置、检索和更新，PDP 负责隐私授权决策的产生，PEP 负责授权决策的执行。在决策过程中，PIP 收集一些属性值，比如服务的信任度。环境处理者管理系统中各组件间的数据交换，IM 管理服务的信任度和隐私敏感度，并提供信任度查询功能。图 6 描述了隐私策略执行系统的体系结构，其中实线部分是 XACML 的标准组件[9]，本文扩展的信息管理组件用虚线表示。

在上述系统中，各功能组件相互交互，协作地进行隐私授权决策。详细的流程如下：

(1)首先，PAP 向策略库中输入隐私访问控制策略。

(2)请求者向 PEP 发送访问请求；PEP 获得该请求，并将请求发送给环境处理者；环境处理者将请求转换成标准的格式，并将转换后的请求发送给 PDP，让它进行授权决策评判。

(3)PDP 获得评判请求后，一方面对策略库进行查找，获得相应的授权策略；另一方面请求环境处理者查询服务的信任度和请求隐私数据集的敏感度，环境处理者将信任度查询请求发送给 PIP。

(4)PIP 对 IM 进行查询，获得信任度和敏感度后，将结果返回给环境处理者；环境处理者再将它转发给 PDP。

(5)PDP 根据隐私授权策略、服务的信任度和隐私数据集的敏感度进行授权决策，并将决策结果发送给环境处理者；环境处理者获得决策结果以后，将其转换成 PEP 的本地格式，并返回给 PEP。

(6)最后，PEP 判定授权决策是否有误，如果没有错误，则执行授权决策，并将结果回复给请求者。

(7)在返回的决策结果中带上相应的义务信息。

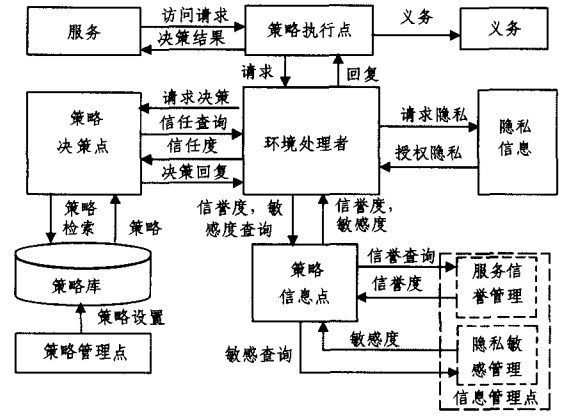

图 6　隐私策略执行系统体系结构

根据以上的描述，给出 PDP 进行隐私授权决策算法的详细步骤。

(1)设 s 和 a 分别为服务以及该服务的一个操作，s 的信誉度为 cr，s 获取的请求者 req 的隐私敏感度为 pr。

(2)获取隐私权限矩阵 c，其中 c 的行数和列数分别为 $|T|$ 和 $|O|$ 与调节因子 β。

(3)由服务的信誉度 cr 和隐私权限矩阵 c，根据公式 $|s.cr-s_i.cr|<\beta$ 计算出服务 s 被授予的相应的角色 $Role_i$，其中 $0<i<n$；依据隐私权限矩阵 $c[i,j]$，判断 $c[i,j]$ 的值，如果为 0，则拒绝访问；如果为 1，则授权访问。

(4)最后判断请求者的隐私敏感度 pr 是否满足 $c[i,j]=1$，如果满足，则服务授权访问用户隐私信息，否则拒绝访问。

算法代码如下所示：

```
1. Input: s;a;
2. Output:true;false;
3. cr:=SR(s);//获得服务 S 的信誉度;
4. pr:=Fp(req);//获取用户隐私敏感度;
5. c:=Fcm(si,pj);β;//获取隐私权限矩阵;
6. For(each i in cm.|T|){ //服务授予相应的角色;
7.      If(|s.cr−si.cr|<β)
8.          s:=Rolei;}
9. For(each j in cm.|O|){ //进行授权判断;
10.   If(pr==Fp(Pj)){
11.    If(c[i,j]==1){
12.      Return true;
13. }}
14. Else{
15.   Return false;}
```

上述算法的时间复杂度为 $O(n)$，其中 n 为角色的个数或隐私数据集的个数。

5　案例分析

考虑一个 Web 服务网上商城的应用，用户 Lily 需要在某网上商城 Box_Store 购买某件商品，并且需要将商品寄送到某地，如果需求能够得到满足，服务提供者需要获取用户的姓

名(Name)、电话号码(Tel)、住址(Addr)和银行卡号(Credit-Card-Num)等隐私数据,根据3.3节的计算隐私数据集敏感度的方法可以得出{Name,Tel,Addr,Credit-Card-Num}的隐私敏感度为4.47。通过3.1节和3.2节可以得到Box_Store的信誉度值为2.298,Box_Store的信誉度值在服务中排列第一(案例中只选择3个服务作为研究对象,实际中服务的数量很大)。

该服务在隐私授权流程中形成的访问控制策略AC如下所示:

Box_Store WITH *Box_Store.credit* GET $role_1$ CAN *read* ON *Lily_info* WITH *Lily_info.sensitivity* FOR *service_release* WITH {*Notify*(*ByEmail*)} IF {sp_1. *credit satisfy Alice_info.Sensitivity*}

当用户Lily向服务Box_Store提交购买商品请求时,Box_Store向代理服务器请求访问用户Lily的隐私数据。详细的流程如下所示:

(1)首先,PAP向策略库中输入隐私授权策略AC。

(2)Box_Store向PEP发送访问请求;PEP获得该请求,并发送给环境处理者;环境处理者将请求转换成标准的格式,并发送给PDP,进行授权决策评判。

(3)PDP获得评判请求后,一方面对策略库进行查找,获得相应的授权策略AC;另一方面请求环境处理者查询Box_Store的信任度和请求{Name,Tel,Addr,Credit-Card-Num}的敏感度,环境处理者将查询请求发送给PIP。

(4)PIP对IM进行查询,获得信任度和敏感度后,将结果返回给环境处理者;环境处理者再将它转发给PDP。

(5)PDP根据隐私授权策略AC、Box_Store的信任度和{Name,Tel,Addr,Credit-Card-Num}的敏感度进行授权决策,并将决策结果发送给环境处理者;环境处理者获得决策结果以后,将其转换成PEP的本地格式,并返回给PEP。

(6)最后PEP判定授权决策是否有误,如果没有错误,则执行授权决策并将是否可以访问Lily隐私信息的结果回复给Box_Store。

(7)在返回的决策结果中带上相应的义务信息。

由于Box_Store的信誉度值很高,根据设置Box_Store可以被授权$Role_1$。根据图7可以看到,$Role_1$能够获取敏感度值最高的隐私数据项,即Box_Store能获取到Lily的{姓名,电话号码,住址,银行卡号}隐私信息。因此,Box_Store可以向Lily提供可信的服务,同时,Lily也可以放心地使用Box_Store提供的服务。

	$Role_1$	$Role_2$	$Role_3$	…	$Role_n$
{Name,Tel,Addr,Credit-Card-Num}	1	0	0	…	0
{Name,Tel,Credit-Card-Num}	1	1	0	…	0
{Tel,Addr,Credit-Card-Num}	1	1	1	…	0
⋮	⋮	⋮	⋮		⋮
{Name,Addr}	1	1	1	…	1

图7 隐私权限矩阵实例

从案例中可以发现,使用隐私访问控制对服务访问用户隐私信息进行控制,解决了常规的访问控制模型由于缺少相关的隐私属性无法精确地执行隐私访问控制策略而不能够完全用于保护用户的隐私信息的问题;只有当服务提供者达到一定的信誉度,能够完全执行策略的要求时,如申明目的、执行义务,服务器端才会将用户的隐私信息提交给服务提供者,可以直接从根源上对服务提供者的隐私信息使用权限进行约束。这避免了服务提供者在获取到用户的隐私信息后,服务提供者的实际操作可能会有意或者无意地违背发布在他们网站上的隐私策略,从而泄漏用户的隐私数据。

6 相关工作

目前,很多研究者已经将访问控制用于隐私保护领域。Waleed W. Smari等人通过扩展ABAC模型,增加了客体和主体,引入了隐私和信任问题,使得访问控制策略对跨组织的协作环境具有敏感性[14];复旦大学刘逸敏等人提出构建基于purpose的对XML数据模式的隐私访问控制策略模型,解决了由路径传递引起的查询隐私数据泄漏问题[15];Mohamed Nabeel等人在DaaS模型中提出了一个CloudMask系统,其为用户将隐私数据保存在云服务中受益,同时为支持对托管在云服务中的共享数据进行细粒度和灵活的访问控制奠定了基础[16];Sushmita Ruj等人针对云计算环境下隐私数据的披露问题,提出了一种云计算下数据隐私保护授权访问控制模式,该模式可以无需知道用户的身份而验证用户的真实性,并使用访问控制技术保证只有有效的用户才可以解密存储信息,该模式防止了对数据的不断攻击和修改[17];Hassan Takabi等人提出了一种数据共享访问控制系统,该系统对存储在云服务提供者(CSP)端的数据提供两层隐私保护,用户的数据通过CSP-enforced访问控制机制防止未授权用户访问,保护CSP对数据的访问是通过多层交换加密与第三方服务提供者的帮助[18];Mohamed Nabeel等人提出了一种细粒度的隐私保护授权访问控制方法,该方法基于密钥管理,当用户的属性满足一定策略时,他才可以访问数据,该方法在将访问控制执行授权给云服务的同时,保护了云数据和云用户隐私的机密性[19];与此同时,一些研究者已经意识到访问控制随着策略不断增加会带来冲突,Qun Ni等人针对访问控制模型中存在的策略冲突问题,提出了冲突检测算法[3];Yoonjeong Kim等人在Qun Ni的基础上提出了新的策略冲突检测算法[20]。

结束语 本文首先提出了基于RBAC的隐私访问控制模型,给出了模型的形式化描述和隐私策略规则的定义;然后分别提出了一种评估服务信誉度和隐私敏感度的方法,利用上述方法可以准确地评估出服务的信誉度和隐私敏感度;最后,在XACML的基础上,扩展了XACML的基本组件,提出了隐私授权决策流程,详细介绍了如何通过基于RBAC的访问控制将隐私信息授权给服务,并给出了案例分析。本文的下一步工作首先是对服务的信誉度进行动态的评估,增加时间因子,以保证服务在不断变化的过程中具有实时的信誉度值;其次是将基于角色的访问控制应用于服务组合中,通过对隐私信息的访问控制动态地组合Web服务。

参考文献

[1] Cranor L F. Platform for privacy preferences (p3p)[M]// Encyclopedia of Cryptography and Security. Springer US, 2011: 940-941

[2] Ashley P, Hada S, Karjoth G, et al. Enterprise privacy authorization language (EPAL 1.2)[Z]. Submission to W3C, 2003

(下转第185页)

李顺东,王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报,2013,41(4):798-803

[9] Schoenmakers B, Tuyls P. Practical two-party computation based on the conditional gate[M]// Advances in Cryptology-ASIACRYPT 2004. Springer Berlin Heidelberg, 2004:119-136

[10] Fagin R, Naor M, Winkler P. Comparing information without leaking it [J]. Communications of the ACM, 1996, 39(5):77-85

[11] Jakobsson M, Yung M. Proving Without Knowing : On Oblivious, Agnostic and Blindfolded Provers[C]// Proceedings of Advances in Cryptology-CRYPTO'96. Springer-Verlag, 1996: 186-200

[12] Boudot F, Schoenmakers B, Traoré J. A Fair and Efficient Solution to the Socialist Millionaires' Problem [J]. Discrete Applied Mathematics, 2001, 111(1):23-36

[13] Qin Jing, Zhang Zhen-feng, Feng Deng-guo, et al. A protocol of comparing information without leaking [J]. Journal of Software, 2004, 15(3):421-427(in Chinese)
秦静,张振峰,冯登国,等. 无信息泄露的比较协议[J]. 软件学报,2004,15(3):421-427

[14] Liu Wen, Luo Shou-shan, Chen Ping. Solution to SMP Based on Sliding Window and Commutation Encryption Function [J]. Computer Engineering, 2007, 33(22):163-171(in Chinese)
刘文,罗守山,陈萍. 基于滑动窗口和交换加密函数解决 SMP 的新方案[J]. 计算机工程,2007,33(22):163-171

[15] Xiao Qian, Luo Shou-shan, Chen Ping, et al. Research on the Problem of Secure Multi-party Ranking Under Semi-honest Model[J]. Acta Electronica Sinica, 2008, 36(4):709-714(in Chinese)
肖倩,罗守山,陈萍,等. 半诚实模型下安全多方排序问题的研究[J]. 电子学报,2008,36(4):709-714

[16] Liu Wen, Wang Yong-bin. Secure multi-party comparing protocol and its applications[J]. Acta Electronica Sinica, 2012, 40(5): 871-876(in Chinese)
刘文,王永滨. 安全多方比较相等协议及其应用[J]. 电子学报,2012,40(5):871-876

[17] Goldreich O. The Fundamental of Cryptography: Basic Applications[M]. London: Cambridge University Press, 2004

[18] Goldreich O. Secure multi-party computation(Manuscript. Preliminary version)[Z]. 1998

(上接第 171 页)

[3] Ni Q, Bertino E, Lobo J, et al. Privacy-aware role-based access control[J]. ACM Transactions on Information and System Security (TISSEC), 2010, 13(3):24

[4] Ardagna C A, Cremonini M, De Capitani di Vimercati S, et al. A privacy-aware access control system[J]. Journal of Computer Security, 2008, 16(4):369-397

[5] Ardagna C A, Damiani E, di Vimercati S D C, et al. Towards privacy-enhanced authorization policies and languages[M]// Data and Applications Security XIX. Springer Berlin Heidelberg, 2005:16-27

[6] Kolter J, Schillinger R, Pernul G. A privacy-enhanced attribute-based access control system[C]// Proc. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security. Edondo Beach, CA, USA, July 2007

[7] Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security (TISSEC), 2001, 4(3):224-274

[8] Ferraiolo D, Cugini J, Kuhn D R. Role-based access control (RBAC): Features and motivations[C]// Proceedings of 11th Annual Computer Security Application Conference. 1995:241-248

[9] Anderson A. A comparison of two privacy policy languages: EPAL and XACML[C]// Proceedings of the 3rd ACM Workshop on Secure Web Service. 2005

[10] Ardagna C A, Cremonini M, De Capitani di Vimercati S, et al. A privacy-aware access control system[J]. Journal of Computer Security, 2008, 16(4):369-397

[11] Ke Chang-bo, Huang Zhi-qiu, Tang Mei. Supporting negotiation mechanism privacy authority method in cloud computing[J]. Knowledge-Based Syst., 2013, 51:48-59

[12] Lv Fu-jun. Web Services Reputation Evaluation Model Based on QoS and User Recommendation[D]. Qinghuangdao: Yanshan University, 2010(in Chinese)
吕福军. 一种基于 QoS 与用户推荐的 Web 服务信誉度评价模型[D]. 秦皇岛:燕山大学,2010

[13] Liu Lin-yuan. Research on Privacy Analysis and Verification of Web Service Composition [D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2011(in Chinese)
刘林源. Web 服务组合隐私分析与验证研究[D]. 南京:南京航空航天大学,2011

[14] Smari W W, Clemente P, Lalande J F. An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system[J]. Future Generation Computer Systems, 2014, 31:147-168

[15] Liu Yi-min, Wang Zhi-hui, Wang Wei. Research and Implementation of purpose-Based Privacy Access Control Policy in XML Data Mode[J]. Computer Applications and Software, 2013, 30(2):148-151(in Chinese)
刘逸敏,王智慧,汪卫. XML 数据模式下基于 purpose 的隐私访问控制策略研究与实现[J]. 计算机应用与软件,2013,30(2):148-151

[16] Nabeel M, Bertino E, Kantarcioglu M, et al. Towards privacy preserving access control in the cloud[C]// 2011 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). IEEE, 2011:172-180

[17] Ruj S, Stojmenovic M, Nayak A. Privacy preserving access control with authentication for securing data in clouds[C]// 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid). IEEE, 2012:556-563

[18] Takabi H. Privacy aware access control for data sharing in cloud computing environments[C]// Proceedings of the 2nd International Workshop on Security in Cloud Computing. ACM, 2014: 27-34

[19] Nabeel M, Bertino E. Privacy preserving delegated access control in the storage as a service model[C]// 2012 IEEE 13th International Conference on Information Reuse and Integration (IRI). IEEE, 2012:645-652

[20] Kim Y, Song E. Privacy-aware role based access control model: Revisited for multi-policy conflict detection[C]// 2010 International Conference on Information Science and Applications (ICISA). IEEE, 2010:1-7