计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20131906
52(4):879-888, 2015

云计算环境下隐私需求的描述与检测方法

柯昌博[1,3]　　黄志球[2]
[1](南京邮电大学计算机学院、软件学院　南京　210023)
[2](南京航空航天大学计算机科学与技术学院　南京　210016)
[3](江苏省无线传感网高技术研究重点实验室　南京　210003)
(brobo.ke@njupt.edu.cn)

Privacy Requirement Description and Checking Method in Cloud Computing

Ke Changbo[1,3] and Huang Zhiqiu[2]
[1](*School of Computer Science & Technology, School of Software, Nanjing University of Posts and Telecommunications, Nanjing* 210023)
[2](*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing* 210016)
[3](*Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing* 210003)

Abstract Cloud computing has been a computing paradigm to provide services for users. However, it is difficult to control and protect personal privacy information because of its opening, virtualization, multi-tenancy and service outsourcing characters. Therefore, how to prevent user privacy information from being used and propagated in cloud computing illegally has become a research focus. In this work, we propose a semantic-oriented privacy requirement description method and checking mechanism. First of all, we describe the user privacy requirement and privacy policy of service provider based on description logic. Secondly, we address the privacy requirement checking framework. Namely, we build the knowledge base through privacy disclosure assertion of user map to TBox and privacy disclosure assertion of service provider map to ABox, and then reason the TBox and ABox by taking advantage of the Tableau algorithm. In the end, we check whether there are the conflicts between user privacy requirement and privacy policy of service provider through experiment and case analysis. Namely, we build the privacy requirement checking model with Protégé of Stanford University, and prove the consistency of conceptions in model and the satisfiability between the conceptions and the logic axioms with Pellet reasonor. Thereby, the correctness and feasibility of our method is certified.

Key words cloud computing; description logic; privacy property; privacy policy; privacy preference

摘　要　云计算已经成为一种计算范型为用户提供服务,但其开放性、虚拟化和服务外包化的特点使得用户的隐私信息难以控制和保护.以描述逻辑为基础,提出了一种云计算环境下面向语义的隐私需求描述与检测方法.首先,对用户隐私需求与服务提供者的隐私策略进行描述;其次,对两者之间是否存在冲突进行检测,发现满足用户隐私需求的服务;最后,利用 Protégé 本体建模工具对用户的隐私需求和服务提供者的隐私策略进行建模,并利用 Pellet 推理机进行了实验,分别对本体模型中的概念进行一致性检测和对概念与逻辑公理之间的可满足性进行检验,从而证明了此检测方法的正确性与可行性.

收稿日期:2013-12-17;**修回日期**:2014-05-12
基金项目:南京邮电大学引进人才科研启动基金资助(NY214164);国家自然科学基金项目(61272083);南京航空航天大学博士学位论文创新与创优基金项目(BCXJ12-14);中央高校基本科研业务费专项资金

关键词 云计算;描述逻辑;隐私属性;隐私策略;隐私偏好

中图法分类号 TP311

云计算具备按需提供服务,支持普适网络访问、资源池位置独立、资源快速伸缩、费用按使用收取等一系列特点[1];同时,具有服务外包化、虚拟化、分布式、多租户等一系列特点.云计算已经作为一种新型的计算模式为用户提供服务,成为广大学者研究的热点.这些特点提高了云计算的服务质量,减少了计算资源的浪费,如服务外包化可以通过服务组合的方式提高服务的能力和专业化水平[2].但与此同时,用户的隐私信息必须对云计算中的外包服务提供者透明,使得用户对外包服务使用隐私信息以及外包服务之间对用户隐私信息的传播难以控制,进而引发了用户对其自身的隐私信息有可能被暴露而担忧.例如,从 2012 年 3 月 1 日起,Google 实施的新的统一隐私策略在美国多地被用户起诉,被欧盟调查并暂缓实施.根据美国电子隐私信息中心(EPIC)分析,"Google 的新隐私策略没有考虑外包服务对隐私数据的使用以及隐私数据在服务之间传播的设置与管理,无法正确体现用户的隐私需求,并有可能与当地法律相冲突."云计算中的隐私保护问题已经成为新型计算模式研究中的焦点.

隐私最早作为一种"保持个人独处"的人权被提出[3].在信息系统与软件工程领域,隐私保护通常代表个体控制自身信息被他人收集、暴露和维持的能力[4].2002 年由万维网联盟(World Wide Web Consortium, W3C)组织开发了隐私偏好平台(the platform for privacy preferences, P3P)[5].该平台提供了一种标准的、机器可读的隐私策略,将其与用户定义的隐私偏好进行匹配,用户利用匹配结果选择满足隐私偏好的服务;但是 P3P 对隐私需求的描述缺少语义信息,并且此平台仅针对 Web 站点,不支持服务组合环境下的隐私保护.而组成云计算的实体都为服务,都是通过服务组合为用户提供服务的,因此 P3P 不能满足云计算环境下的需求.2005 年结构化信息标准促进组织(Organization for the Advancement of Structured Information Standards, OASIS)提出了访问控制标记语言(extensible access control markup language, XACML)[6].XACML2.0[7] 通过"profile for privacy policies"扩展了对隐私策略的支持.而针对不同的云计算用户群体有不同的隐私需求,对隐私敏感信息的定义也不相同;但是 XACML 的隐私策略仅仅针对服务提供者,没有考虑用户的个人隐私需求,因此,很难保证参与服务组合的服务能够满足用户的隐私需求.文献[8-9]将云计算环境中的隐私保护定义为云服务的用户控制个人敏感信息(personal sensitive information, PSI)被云服务提供者收集、使用、暴露和维持的能力,此研究为云计算隐私保护提供了一定的理论指导,但没有给出具体的隐私保护解决方案.

由于云计算的软件即服务层(software as a service, SaaS)为 Web 服务,本文主要针对云计算服务外包化的特征,采用以描述逻辑为基础提出了隐私需求的描述与检测方法.该方法首先从用户的隐私需求中获取隐私偏好,从服务的输入与前置条件中获取服务提供者的隐私属性集[10];其次,利用形式化的方法定义了隐私属性、服务提供者的隐私披露策略以及用户的隐私偏好与隐私披露断言,并对服务双方的隐私需求进行冲突检测,找出待协商的隐私属性序列;最后,利用实验证明了此方法的可行性与正确性.

1 相关工作

我们将隐私保护的相关工作以隐私需求的建模与验证、隐私策略的匹配与协商、隐私数据的暴露、风险这 4 个部分进行分类.同时,对这 4 类分别从贡献、所对应的计算范型、是否支持服务组合、所表达的模型或者过程是否拥有语义这 4 个方面使用表格的形式进行了比较分析,如表 1 所示,表 1 参见文献[11-24].

由于我们的工作是对隐私策略的匹配相关,因此重点讨论匹配类中的工作,其他类的工作可以通过表格得出相关的比较结果.文献[15]在分析现有隐私规则的基础上,分别定义了用户和服务提供者的隐私策略,提出了隐私策略自动匹配方法,该方法能对隐私数据的类型、数据暴露的目的、数据的收集者以及维持时间进行检测;但此工作没有服务组合者或者官方对服务提供者是否授权进行描述和匹配,使得用户的隐私数据可能在非授权的服务提供者之间进行传播,提高了用户隐私数据被非法暴露的风险.文献[16]对普适计算应用中的隐私保护策略进行了研究,使用多类逻辑和描述逻辑建立了隐私策略模型和隐私策略公理,并给出了隐私策略的

逻辑推理方法,能检测出策略之间的不一致.而云计算中的实体都为服务,并在虚拟环境下使用服务组合为用户提供应用,但此工作不支持服务组合,因此很难应用于云计算中的隐私保护.我们的工作是以描述逻辑为基础,对云计算环境下的服务组合进行隐私检测,得到满足用户隐私需求的服务集和待协商的隐私属性序列,为我们团队实现基于问责制的云计算隐私保护提供理论支持.

Table 1 Comparison of Related Works
表 1 相关工作之间的比较

Methods	Reference	Contributions	Computing Paradigm	Support for Service Composition	Support for Semantic
Modeling and Verification	Ref.[11]	Conceptual Modeling of Privacy-aware Web Service	Service Computing	×	√
	Ref.[12]	Privacy-aware Web Service Protocol Replaceability	Service Computing	×	√
	Ref.[13]	Verification of Privacy Timed Properties	Service Computing	×	×
	Ref.[14]	Minimal Privacy Authorization in Web Services Collaboration	Service Computing	√	×
Matching	Ref.[15]	Privacy and Utility in Business Processes	Service Computing	√	√
	Ref.[16]	Privacy-Protection Policy for Pervasive Computing	Pervasive Computing	×	√
	Our Work	Privacy Requirement Description and Checking Method in Cloud Computing	Cloud Computing	√	√
Negotiation	Ref.[17]	Role-based Collaboration and its Kernel Mechanisms			×
	Ref.[18]	A Privacy Negotiation Protocol for Web Services	Service Computing	×	×
	Ref.[19]	Parsimonious Semantic Trust Negotiation			√
	Ref.[20]	Supporting Negotiation Mechanism Privacy Authority Method in Cloud Computing	Cloud Computing	√	√
Disclosure	Ref.[21]	Visualizing Past Personal Data Disclosures	Service Computing	×	×
	Ref.[22]	Analysis of the Minimal Privacy Disclosure	Service Computing	√	×
Risk	Ref.[23]	Modeling and Measuring Privacy Risks	Service Computing	√	×
	Ref.[24]	Privacy Risk Models	Pervasive Computing	×	√

Notes: √: Support; ×: Not support.

2 隐私属性的描述

2.1 服务方的隐私属性描述

我们通过与知识领域本体之间的映射得到隐私属性之间的关系,然后利用本体树进行描述.隐私属性的本体树如图1所示,其中 Thing 为根节点,是所有隐私属性类的超类;除底层之外其他各层之间是类与子类的关系即包含关系,例如 *Name* 类包含 *realName* 和 *nickName*;只有底层与其上层是属于关系,例如 *country*, *province*, *city* 是属于 *address* 类.

定义 1. 服务方的隐私属性 *PA-S*(privacy attribute of service).隐私属性可以用一个五元组表示,即 $PA\text{-}S=\langle Issuer, Owner, Subject, PDA\text{-}S, Signature\rangle$.其中,*Issuer* 表示隐私属性的标识,

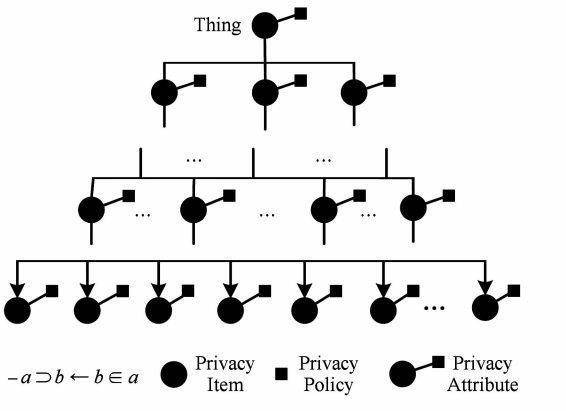

Fig. 1 Ontology description of privacy property.

图 1 隐私属性的本体描述

记录此隐私属性类的父类与子类；*Owner* 表示服务组合的参与者，同时也是隐私属性的拥有者；*Subject* 为某一隐私属性的名字；*PDA-S*（privacy disclosure assertion of service）为隐私披露断言；*Signature* 为数字签名. 每一个隐私属性对应隐私属性本体中的一个概念. *Subject* 可以表示为

$$Subject = C(op_1:I_1, op_2:I_2, op_3:I_3, \cdots, op_n:I_n) \vee C(dp_1:D_1, dp_2:D_2, dp_3:D_3, \cdots, dp_n:D_n),$$

其中，C 为表示隐私本体中的类；op_i 和 dp_i 分别表示类中所具有的对象属性和数据属性，并且满足 $\forall (i \neq j) \rightarrow (op_i \neq op_j) \wedge (dp_i \neq dp_j)$；$I_i$ 表示某一隐私本体中的实例对象；D_i 是某一确定数值或常量.

定义 2. 委托授权声明（delegation of authority statement，*DAS*）. 委托授权声明是隐私披露断言的一部分，即每一个隐私属性的披露都要满足委托授权声明以证实服务参与者是否拥有此隐私属性的权限. *DAS* 可表示为

$$DAS:[(serverConstr \otimes authorizer) \Leftarrow assertion].$$

假若：

$$authorizer = \{official, serviceComp\},$$

其中，*official* 表示官方组织；*serviceComp* 表示服务组合者；*serverConstr* 表示官方或者服务组合者对服务参与者在规章制度或者法律上的约束，例如 *EBay* 电子商务平台. 委托授权声明明确了服务参与者必须满足断言表达式 *assertion*，并且有效的委托授权声明必须包含官方或服务组合者对该断言的签名，同时将此签名放入隐私属性中.

例 1. *EBay* 发布的委托授权声明称：假如为 *EBay* 的 *VIP* 用户，必须声誉值大于 600 或者拥有银行 *Bank* 的额度大于 6000 的信用卡用户，此委托授权声明可以表示为

$$VIP \otimes EBay \Leftarrow credit[>6000(rating)] \otimes Bank \vee reputation[>600(value)] \otimes EBay. \quad (1)$$

定义 3. 隐私披露断言（privacy disclusure assertion of service，*PDA-S*）. 隐私披露断言是指针对某一服务参与者对拥有某一隐私属性的一个约束断言，可表示为

$$PDA\text{-}S = subjConstr \Theta ownerConstr;$$
$$subjConstr = C(op_1:\{ow_1, \cdots, ow_n\}, \cdots, op_n:\{ow_1, \cdots, ow_n\}) \wedge C(op_1:ow_1(vt_1), \cdots, op_n:ow_n(vt_n));$$
$$ownerConstr = DAS.$$

隐私披露断言 *PDA-S* 由 2 部分组成，即对隐私属性内容的约束（*subjConstr*）和对拥有此隐私属性的服务参与者的约束（*ownerConstr*）.

SubjConstr 主要是对服务参与者是否拥有该隐私属性，以及该服务参与者使用此隐私属性的有效时间进行约束. C 表示隐私属性类，指明服务参与者与用户进行隐私属性交换时只能对其所对应的类或子类进行交换；$op_1:\{ow_1, \cdots, ow_n\}$ 中 op_1 表示此类的某个实例，$\{ow_1, \cdots, ow_n\}$ 表示此实例所对应的服务参与者；$op_1:\{ow_1, \cdots, ow_n\}, \cdots, op_n:\{ow_1, \cdots, ow_n\}$ 表示隐私属性类的实例可以被那些服务参与者拥有；$op_1:ow_1(vt_1), \cdots, op_n:ow_n(vt_n)$ 表示服务参与者对此隐私属性实例有效的使用时间，同时，若 vt_i 的数据域为整数域，那么 ow_i 为建立在 vt_i 的数据域上的一个一元谓词，常见的谓词为 $\geqslant a$ 或者 $\leqslant a$，其中 a 为常量.

ownerConstr 是对拥有隐私属性的服务参与者的约束，*ownerConstr*=*DAS*，表示服务参与者在拥有此隐私属性时必须满足官方或者服务组合者的委托授权声明.

例 2. 家具公司 *A* 想在 *EBay* 申请一个网络商品，出售一批家具 Furniture，而 *EBay* 针对用户地址的隐私披露断言为：假如家具公司 *A* 为 *EBay* 的 *VIP* 用户. *EBay* 要求只能把买家的地址披露给快递公司，并要求在交易成功并组织派送后 2 h 内删除. 此时，隐私披露断言可以表示如下：

$$address:shipper \wedge [address:\leqslant 2h(vt) \Theta Seller:VIP \otimes EBay]. \quad (2)$$

将式(1)代入式(2)可得：

$$address:shipper \wedge \{address:\leqslant 2h(vt) \Theta credit[>6000(rating)] \otimes Bank \vee reputation[>600(value)] \otimes EBay\}. \quad (3)$$

定义 4. 隐私披露策略(privacy discloser strategy, *PDS*).隐私披露策略为隐私披露断言的一个有序序列,即

$$PDS=PDA\text{-}S_1 \wedge PDA\text{-}S_2 \wedge \cdots \wedge PDA\text{-}S_n.$$

2.2 用户方的隐私属性描述

定义 5. 用户方的隐私属性(privacy attribute of user, *PA-U*).用户方的隐私属性与服务方的隐私属性描述方法相似,也可以用一个五元组表示,即

$$PA\text{-}U = \langle Issuer, Service, Subject, PDA\text{-}U, Signature\rangle,$$

其中,*Issuer* 表示隐私属性的标识,记录此隐私属性类的父类与子类;*Service* 表示用户对个人的隐私信息所暴露的对象;*Subject* 为某一隐私属性类的主题;*PDA-U*(privacy disclosure assertion of user)为隐私暴露断言;*Signature* 为数字签名. *Subject* 的表示方式与定义 1 服务方的隐私属性中的 *Subject* 相同.

定义 6. 隐私暴露断言(privacy disclosure assertion of user, *PDA-U*).隐私暴露断言是指针对某一服务提供者对拥有某一隐私属性的一个约束断言,可表示为

$$PDA\text{-}U = subjConstr\Theta serverConstr;$$

$$subjConstr = C(op_1:\{ow_1,\cdots,ow_n\},\cdots, op_n:\{ow_1,\cdots,ow_n\}) \wedge C(op_1:ow_1(vt_1),\cdots,op_n:ow_n(vt_n));$$

$$serverConstr = trustDegree.$$

隐私暴露断言 *PDA-U* 由 2 部分组成,即对隐私属性内容的约束(*subjConstr*)和对拥有此隐私属性的服务提供者的约束(*serverConstr*).前者 *subjConstr* 的表示与定义 3 中的 *subjConstr* 相同;后者 *serverConstr* 是由用户对服务或者服务提供者的认可程度(*trustDegree*)所决定.认可程度可以表示为 $trustDegree=\{S, DAS, Re\}$,其中 *S* 表示安全性(security),用来保证数据的真实性、完整性以及服务质量(quality of service, QOS)的可信性;*DAS* 是指服务或者服务提供者所拥有的委托授权声明;*Re* 表示服务或者服务提供者的声誉(reputation).委托授权声明 *DAS* 包含官方或者服务组合者对服务提供者所颁发的委托授权声明,例如 *Seller* 是否为 *VIP* 用户,快递公司或者银行是否拥有官方颁发的经营许可证等(本文假设所有的快递公司和银行都拥有官方颁发的经营许可证).

定义 7. 隐私偏好(privacy preference, *PP*).隐私偏好为隐私暴露断言的一个有序序列,即:

$$PP = PDA\text{-}U_1(C_1(op_1)) \wedge PDA\text{-}U_2(C_2(op_2)) \wedge \cdots \wedge PDA\text{-}U_n(C_n(op_n)).$$

例 3. Tom 要求家具公司 *A* 最好为 *EBay* 的 *VIP* 用户.在交易过程中,Tom 只想将自己真实的名字(*realName*)和手机号码(*mobilephoneNumber*)暴露给 *EBay* 的 *VIP* 用户,非 *VIP* 用户只能暴露自己的笔名(*nickName*)和办工室电话号码(*officephoneNumber*);银行卡号(*creditCard*)只能提供给银行(*Bank*);地址(*address*)和邮编(*zipCode*)只能提供给快递公司(*Shipper*)或邮局(*Postoffice*);在交易完成后,*EBay* 和所有服务参与方必须在 20 min 内自动清除所有隐私信息.此隐私暴露策略如表 2 所示:

Table 2 Instances of Privacy Disclosure Assertion

表 2 隐私暴露断言的示例

Privacy Requirements	Privacy Disclosure Assertion(*PDA-U*)
realName can only be provided to *VIP* seller of *EBay*.	$PDA\text{-}U_1$ $realName$:[$Seller$:$VIP\otimes EBay$].
mobilephoneNumber can only be disclosed to *VIP* seller of *EBay*.	$PDA\text{-}U_2$ $mobilephoneNumber$:[$Seller$:$VIP\otimes EBay$].
nickName or *officephoneNumber* can be provided to non-*VIP* seller of *EBay*.	$PDA\text{-}U_3$ $nickName \vee officephoneNumber$:[$Seller$:$\neg VIP \otimes EBay$].
creditCard can only be provided to *Bank*.	$PDA\text{-}U_4$ $creditCard$:$Bank$.
address and *zipCode* can only be provided to *Shipper* or *Postoffice*.	$PDA\text{-}U_5$ $address \wedge zipCode$:$shipper \vee postoffice$.
Once transaction is done, *EBay* and all parts must delete all privacy information within 20 min.	$PDA\text{-}U_6$ $success \wedge [allPA:\leqslant 20\min(vt)]$.

因此,隐私偏好为

$$PP = PDA\text{-}U_1(realName) \wedge PDA\text{-}U_2(phoneNumber) \wedge PDA\text{-}U_3(nickName \vee officephoneNumber) \wedge PDA\text{-}U_4(creditCard) \wedge PDA\text{-}U_5(address \wedge zipCode) \wedge PDA\text{-}U_6(allPA).$$

为了容易理解用户的隐私需求和服务提供者的隐私策略,且方便简捷地描述隐私属性和隐私策略

断言,我们采用了上述隐私协商语言 PNL 语法的表达方式. PNL 是以描述逻辑为基础,因此,每个隐私属性中的类、对象和数据分别对应描述逻辑中的一个概念、角色和特征. 我们设计了描述逻辑的转化函数(privacy description logic function):$PDL()$,转化关系如下所示:

1) $serverConstr \otimes authorizer \rightarrow serverConstr \sqcap authorizer$;

2) $PDA_1 \vee PDA_2 \rightarrow PDL(pda_1) \sqcup PDL(pda_2)$;

3) $PDA_1 \wedge PDA_2 \rightarrow PDL(pda_1) \sqcap PDL(pda_2)$;

4) $(pda) \rightarrow (PDL(pda))$;

5) $subjConstr \Theta ownerConstr \rightarrow \exists hasID.(PDL(subjConstr)) \sqcap \exists authorizerIs.PDL(ownerConstr))$;

6) $subjConstr \Theta serverConstr \rightarrow \exists hasID.(PDL(subjConstr)) \sqcap \exists userIs.PDL(serverConstr))$;

7) $C(op_1:\{ow_1,\cdots,ow_n\},\cdots,op_n:\{ow_1,\cdots,ow_n\}) \wedge C(op_1:ow_1(vt_1),\cdots,op_n:ow_n(vt_n)) \rightarrow C \sqcap (\exists op_1\{ow_1,\cdots,ow_n\} \sqcap \cdots \sqcap \exists op_n\{ow_1,\cdots,ow_n\} \sqcap ow_1(vt_1) \sqcap \cdots \sqcap ow_n(vt_n))$.

3 隐私需求的检测

3.1 隐私需求检测框架

隐私需求检测框架分为隐私需求描述层(privacy requirement description layer)和隐私需求检测层(privacy requirement checking layer)这 2 层,如图 2 所示.

图 2 中带有方格背景的部分为隐私需求描述层. 该层主要完成以下 2 方面的工作:

1) 将用户方的隐私属性 *PA-U* 转为知识库可理解的隐私暴露断言 *PDA-U*;

2) 利用 XML 的路径语言 Xpath 提取服务文档中的输入和前置条件得到服务方隐私属性 *PA-S*,并转为隐私披露断言 *PDA-S*.

图 2 中带有竖线背景的部分为隐私需求检测层. 该层主要利用算法 Tableau 对上层获取的隐私暴露断言和隐私披露断言进行隐私需求检测,最后将检测结果返回给用户.

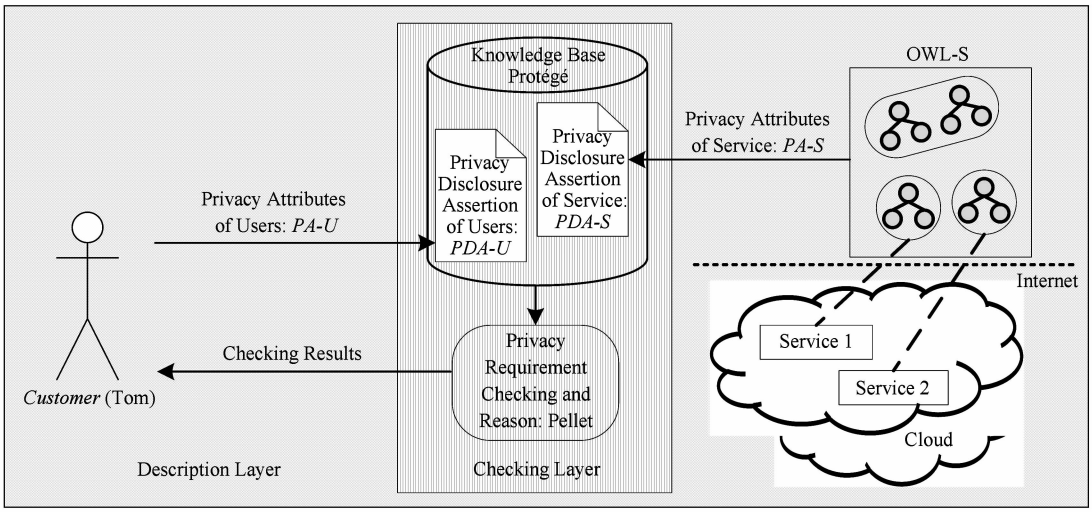

Fig. 2 Detection architecture of privacy requirement.

图 2 隐私需求的检测框架

3.2 隐私需求检测案例与实验分析

Tom 想通过云服务组合者(cloud-service composer, CSC)向 *EBay* 的服务提供者家具公司 *A* 购买一批家具 Furniture,其中家具公司 *A* 为 *EBay* 的非 *VIP* 用户. Tom 对非 *VIP* 用户,如果暴露自己的真实名字(*realName*),则只能暴露自己的办工室电话号码(*officephoneNumber*),并且地址中不能带有社区信息. 名字(*realName*)、不带社区信息的地址(*AddressWithoutCommunity*)和电话号码(*officephoneNumber*)只能提供给快递公司或邮局;在交易完成后,CSC, *EBay* 和所有服务参与方必须在 20 min 内自动清除所有用户隐私信息.

而对于 *EBay* 的非 *VIP* 用户家具公司 *A*,CSC 只允许 *A* 将 Tom 的名字(*realName*)、不带社区信息的地址(*AddressWithoutCommunity*)和电话号码(*officephoneNumber*)提供给快递公司或邮局;在交易完成后,*A* 和所有服务参与方必须在 15 min 内自动清除所有用户隐私信息.

完成此服务涉及到一个云服务组合者 CSC 以及在线购物平台 *EBay*、顾客 *Customer*(Tom)、售货

商 *Seller*(S)、邮局(*Postoffice*)或快递公司(*Shipper*)这 4 个协作单元,其中 *Customer* 的姓名(*name*)、家庭住址(*address*)、邮编(*postcode*)、电话(*phone*)是其个人隐私数据.

交易之初,Tom 向 *Seller* 发送订单请求消息(OrdReq),CSC 向服务参与者收集相关的隐私属性,并向所有的服务参与者发送完成服务所需的相关隐私属性请求消息(PriReq),CSC 收集到所有的隐私属性后,通过隐私协商服务向 Tom 发送隐私属性收集完成的消息;然后,启动双方的隐私协商引擎进行隐私策略的预协商和隐私暴露断言的交换. *Seller* 接收到 OrdReq 和 CSC 的协商成功消息(NegoSucc)后,选择 *Postoffice* 或者 *Shipper* 向 Tom 发送货物(PostReq/ShipReq),到货后(PostEnd/ShipEnd)*Postoffice* 或者 *Shipper* 要求 Tom 支付货款,Tom 收到货物并支付货款后通知 *Seller* 交易完成(PostSucc/ShipSucc). 该案例的交易场景如图 3 所示:

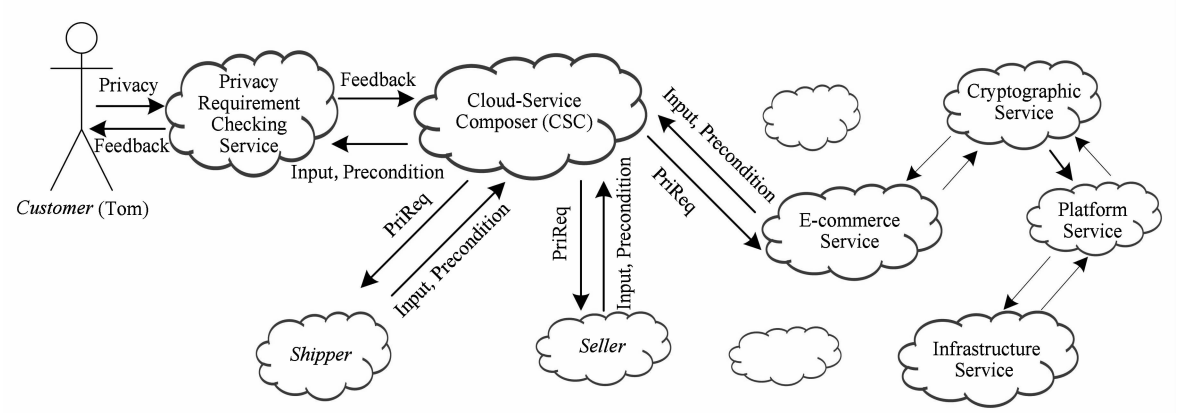

Fig. 3 Online purchase case.

图 3 在线购物案例

我们实验采用的计算机处理器为 Intel® Core™2 Duo CPU 2.20 GHz,内存为 2 GB,操作系统为 Windows 7 32 b. 本体建模工具采用斯坦福大学基于 Java 语言开发的本体编辑工具 Protégé,同

```
E:\test\pellet-2.3.0>pellet classify e:\test\privacy-requirement-checking.owl
Classifying 33 elements
Classifying:  100% complete in 00:00
Classifying finished in 00:00

 owl:Thing
    ontology1358410681710:customer
       ontology1358410681710:man
       ontology1358410681710:woman
    ontology1358410681710:privacy
       ontology1358410681710:ID-Card-Number
       ontology1358410681710:address
          ontology1358410681710:addressWithCommunity
             ontology1358410681710:addressWithoutCommunity
                ontology1358410681710:city
                ontology1358410681710:country
                ontology1358410681710:province
                ontology1358410681710:street
             ontology1358410681710:community
       ontology1358410681710:name
          ontology1358410681710:nickName
             ontology1358410681710:MisFirstName
             ontology1358410681710:MrFirstName
          ontology1358410681710:realName
             ontology1358410681710:firstName
             ontology1358410681710:lastName
             ontology1358410681710:secondName
       ontology1358410681710:phone
          ontology1358410681710:Mobile
          ontology1358410681710:officePhone
       ontology1358410681710:zipCode
    ontology1358410681710:privacyholder
       ontology1358410681710:E-commerceService
       ontology1358410681710:Seller
       ontology1358410681710:bank
       ontology1358410681710:cloudServiceComposer
       ontology1358410681710:shipper
```

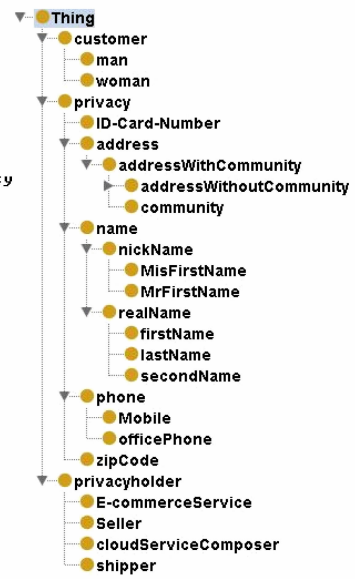

Fig. 4 Classes of privacy conflict detection ontology.

图 4 隐私冲突检测本体中类的结构

时使用美国马里兰大学 Mind Swap 实验室开发的 Pellet 推理机作为冲突检测的验证工具,版本号为 2.3.0.

因此,我们利用 Protégé 对上述购物案例构建隐私冲突检测本体 privacy-conflict-detection.owl,此本体中的概念和实例映射为 Tbox,利用概念、属性和实例定义的用户隐私偏好断言 φ(逻辑公理)映射为 Abox,Tbox 和 Abox 组成了隐私冲突检测知识库;然后,将构建的 privacy-conflict-detection.owl 文件存放在本地机 e 盘的 test 目录下,使用 Pellet 进行推理,具体分以下 4 步:

1) 采用命令 pellet classify e:\test\privacy-requirement-checking.owl 对本体进行分类,得到隐私冲突检测本体中类的结构,如图 4 所示.

2) 通过 Pellet 推理机对隐私冲突本体文件 privacy-conflict-detection.owl 使用命令 pellet info e:\test\privacy-requirement-checking.owl 显示本体文件中的主要信息,如公理 Axioms 为 208 个,其中逻辑公理 Logical Axioms 为 157 个,个体 Individuals 为 20 个,类 Classes 为 32 个,对象属性 Object Properties 为 19 个.显示结果如图 5 所示.

3) 使用命令 pellet consistency e:\test\privacy-requirement-checking.owl 来检测本体文件中概念的一致性.显示结果如图 6 所示,具体为 consistent: yes.通过这个结果,我们可以得到本体映射模型中的概念在语义上是一致的,即在语义上不存在冲突,从而保证了本体概念和逻辑公理之间进行冲突检测所得到的结果的正确性和唯一性.

4) 使用命令 pellet unsat e:\test\privacy-requirement-checking.owl 来检测本体文件中的本体概念与逻辑公理之间的可满足性,即本体概念与概念之间的关系是否满足逻辑公理.显示结果如图 7 所示,具体为 Found no unclassifiable concepts.此结果表明,隐私冲突检测知识库中的服务提供者,即本体文件中的隐私拥有者 privacyHolder 的个体所拥有的隐私概念满足用户的隐私偏好断言 φ,因此证明了用户的隐私偏好与服务提供者的隐私策略之间不存在冲突.

```
E:\test\pellet-2.3.0>pellet info e:\test\privacy-requirement-checking.owl
Information about file:/e:/test/privacy-requirement-checking.owl (<http://www.se
manticweb.org/ontologies/2013/0/Ontology1358410681710.owl>)
OWL Profile = OWL 2 DL
DL Expressivity = ALR
Axioms = 208
Logical Axioms = 157
GCI Axioms = 0
Individuals = 20
Classes = 32
Object Properties = 19
Data Properties = 0
Annotation Properties = 0
```

Fig. 5 Main information of ontology model.

图 5 本体模型中的主要信息

```
E:\test\pellet-2.3.0>pellet consistency e:\test\privacy-requirement-checking.owl

Consistent: Yes

E:\test\pellet-2.3.0>
```

Fig. 6 Consistent checking of conception in ontology model.

图 6 本体文件中概念的一致性

```
E:\test\pellet-2.3.0>pellet unsat e:\test\privacy-requirement-checking.owl
Finding unsatisfiable 31 elements
Finding unsatisfiable:  100% complete in 00:00
Finding unsatisfiable finished in 00:00

Found no unsatisfiable concepts.
```

Fig. 7 Satisfiability between ontology conception and logical axioms.

图 7 本体概念与逻辑公理之间的可满足性

4 结论与进一步工作

本文提出了一种基于描述逻辑的隐私需求与隐私策略的描述方法,通过此描述方法可以实现面向语义的隐私需求检测推理,得到满足用户隐私需求的服务,同时也可以得到检测后的隐私属性序列,为下一步工作隐私合同的协商打下理论基础.因此,我们的下一步工作是在假设没有满足用户隐私需求的服务时提出一种协商机制,通过协商得到满足用户与服务提供者双方的隐私合同.

参 考 文 献

[1] Mell P, Grance T. Draft NIST working definition of cloud computing [EB/OL]. Washington: Information Technology Laboratory, United States Department of Commerce, 2010 [2014-04-08]. http://csrc.nist.gov/groups/SNS/cloud-computing

[2] Armbrust M, Fox A, Griffith R, et al. Above the clouds: A berkeley view of cloud computing, UCB/EECS-2009-28 [R]. Berkeley, CA: University of California, Berkeley, 2009: 1-23

[3] Caroline K, Ellen A. The Right to Privacy [M]. New York: Vintage, 1972: 100-132

[4] Goldberg I, Wagner D, Brewer E. Privacy-enhancing technologies for the Internet [C] //Proc of the 42nd IEEE Int Computer Conf (COMPCON'97). Piscataway, NJ: IEEE, 1997: 103-109

[5] Xiao Fangxiong, Huang Zhiqiu, Cao Zilin, et al. Modeling cost-aware Web services composition using PTCCS [C] //Proc of the 2009 IEEE Int Conf on Web Services (ICWS 2009). Piscataway, NJ: IEEE, 2009: 461-468

[6] Yee G, Korba L. Privacy policy compliance for Web services [C] //Proc of the 2004 IEEE Int Conf on Web Services(ICWS 2004). Piscataway, NJ: IEEE, 2004: 158-165

[7] Zhang Jia, Chang Carl K, Zhang Liangjie, et al. Toward a service-oriented development through a case study [J]. IEEE Trans on Systems, Man, Cybernetics: Part A, 2007, 37 (6): 955-969

[8] Pearson S. Taking account of privacy when designing cloud computing services, HPL-2009-54 [R]. Palo Alto, CA: HP Labs, 2009

[9] Pearson S, Charlesworth A. Accountability as a way forward for privacy protection in the cloud, HPL-2009-178 [R]. Palo Alto, CA: HP Labs, 2009

[10] Ke Changbo, Huang Zhiqiu. Self-adaptive semantic Web service matching method [J]. Knowledge-Based System, 2012, 35: 41-48

[11] Hamadi R, Paik H, Benatallah B. Conceptual modeling of privacy-aware Web service protocols [C] //Proc of the 19th Int Conf on Advanced Information Systems Engineering (CAiSE'07). Berlin: Springer, 2007: 233-248

[12] Guermouche N, Benbernou S, Coquery E, et al. Privacy-aware Web service protocol replaceability [C] //Proc of the 2007 IEEE Int Conf on Web Services (ICWS 2007). Piscataway, NJ: IEEE, 2007: 1048-1055

[13] Mokhtari K, Benbernou S, Hacid M, et al. Verification of privacy timed properties in Web service protocols [C] //Proc of the 2008 IEEE Int Conf on Services Computing (SCC 2008). Piscataway, NJ: IEEE, 2008: 593-594

[14] Liu Linyuan, Zhu Haibin, Huang Zhiqiu et al. Minimal privacy authorization in Web services collaboration [J]. Computer Standards & Interfaces, 2011, 33(3): 332-343

[15] Barth A, Mitchell J, Datta A, et al. Privacy and utility in business processes [C] //Proc of the 20th IEEE Computer Security Foundations Symp (CSF 2007). Piscataway, NJ: IEEE, 2007: 279-294

[16] Wei Zhiqiang, Kang Mijun, Jia Dongning, et al. Research on privacy-protection policy for pervasive computing [J]. Chinese Journal of Computers, 2010, 33(1): 128-138 (in Chinese)
(魏志强,康密军,贾东宁,等. 普适计算隐私保护策略研究[J]. 计算机学报, 2010, 33(1): 128-138)

[17] Zhu Haibin, Zhou Mengchu. Role-based collaboration and its kernel mechanisms [J]. IEEE Trans on Systems, Man, Cybernetics: Part C, 2006, 36(4): 578-589

[18] El-Khatib K. A privacy negotiation protocol for Web services [R/OL]. Ottawa, Ontario, Canada: Institute for Information Technology, National Research Council, 2003 [2013-06-12]. http://nparc.cisti-icist.nrc-cnrc.gc.ca/npsi/ctrl?action=rtdoc&an=5765603&lang=en

[19] Zhang Yan, Fen Dengguo. Parsimonious semantic trust negotiation [J]. Chinese Journal of Computers, 2009, 32 (10): 1989-2003 (in Chinese)
(张妍,冯登国. 吝啬语义信任协商[J]. 计算机学报, 2009, 32(10): 1989-2003)

[20] Ke Changbo, Huang Zhiqiu, Mei Tang. Supporting negotiation mechanism privacy authority method in cloud computing [J]. Knowledge-Based Systems, 2013, 51: 48-59

[21] Jan K, Michael N, Günther P. Visualizing past personal data disclosures [C] //Proc of the 17th Int Conf on Availability, Reliability and Security (ARES 2010). Piscataway, NJ: IEEE, 2010: 131-139

[22] Liu Linyuan, Zhu Haibin, Huang Zhiqiu. Analysis of the minimal privacy disclosure for Web services collaborations with role mechanisms [J]. Expert System & Application, 2011, 38(4): 4540-4549

[23] Yu T, Zhang Y, Lin K. Modeling and measuring privacy risks in QoS Web services [C] //Proc of the 8th IEEE Int Conf on E-Commerce Technology (CEC 2006)/the 3rd IEEE Int Conf on Enterprise Computing, E-Commerce and E-Services (EEE 2006). Piscataway, NJ: IEEE, 2006: 4

[24] Jason H, Jennifer D. Landay: Privacy risk models for designing privacy-sensitive ubiquitous computing systems [C] //Proc of the Int Conf on Designing Interactive Systems (DIS 2004). Piscataway, NJ: IEEE, 2004: 91-100

Ke Changbo, born in 1984. PhD and lecturer. His main research interests include security and privacy of information system, cloud computing and ontology-based software engineering.

Huang Zhiqiu, born in 1965. Professor and PhD supervisor. His main research interests include software engineering, cloud computing and formal method.