基于用户同意的隐私保护协议形式化描述与验证

马 丽[1],姜火文[1],彭 云[2]
(1. 江西科技师范大学大数据科学学院,江西南昌 330038;2. 江西师范大学数字产业学院,江西南昌 330022)

摘 要: 将用户同意与访问控制相结合是解决隐私保护的主要方法之一. 然而,现有的隐私保护访问控制方法仅从数据控制者的角度,不考虑个人对访问决策的参与,无法满足自主可控的需求. 为了解决这个问题,本文提出了一种基于用户同意的隐私保护访问控制协议,将用户同意转化为一种同意权限,形成一种同意加授权的双重访问控制机制. 本文给出协议的语法、语义及安全性定义和分析,并采用模型检测的方法对协议应满足的性质进行验证,最终证明本文的设计可以从访问控制的角度满足个人信息保护法规的要求.

关键词: 个人数据保护;隐私保护模型;隐私保护协议;访问控制;隐私授权;TLA+(Temporal Logic of Actions plus)
基金项目: 江西省社会科学基金项目(No.21TQ08D);江西省高校人文社会科学研究项目(No.JC22115);江西省自然科学基金项目(No.20224BAB202013)
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112(2023)07-1842-08
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20230144

Formalization and Verification of Privacy Preserving Protocol Based on User Consent

MA Li[1], JIANG Huo-wen[1], PENG Yun[2]
(1. *School of Big Data Science, Jiangxi Science & Technology Normal University, Nanchang, Jiangxi* 330038, *China*;
2. *School of Digital Industry, Jiangxi Normal University, Nanchang, Jiangxi* 330022, *China*)

Abstract: The combination of user consents and access control is one of the main approaches to address privacy protection today. However, most of privacy protection access control approaches are from the perspective of the data controller, without considering individual participation in access decisions, and can not meet the need for privacy protection in terms of autonomy and control. In order to solve this problem, this paper proposes a privacy-preserving access control protocol based on user consents, which transforms user consents into a kind of consent authority and forms a dual access control mechanism of consent plus authorization. The syntax, semantics and security of the protocol are defined and analyzed. The properties that the protocol should satisfy are verified with the model checking method, which finally proves that the design of this paper can comply with personal information protection regulations from the perspective of access control.

Key words: personal data protecting; privacy preserving model; privacy preserving protocol; access control; privacy authorization; TLA+ (Temporal Logic of Actions plus)
Foundation Item(s): Social Science Foundation Project of Jiangxi Province (No.21TQ08D); Humanities and Social Science Project of University of Jiangxi Province (No.JC22115); Natural Science Foundation of Jiangxi Province of China (No.20224BAB202013)

1 引言

个人数据保护(Personal Data Protection, PDP)法规,如欧盟的通用数据保护条款(General Data Protection Regulations, GDPR)以及我国的个人信息保护法,都规定了数据的处理者在访问个人数据之前应获得数据主体的"同意". 如果把隐私数据视为一类特殊的数据资源,则可以在对这类资源进行访问控制保护时将用户"同意"与访问控制技术结合起来考虑,以满足法律合规性. 目前这项研究已经成为隐私保护领域关注的焦点[1,2].

目前隐私保护访问控制主要基于ABAC(Attribute-Based Access Control)模型和RBAC(Role-Based Access

收稿日期:2023-02-17;修回日期:2023-06-01;责任编辑:覃怀银

Control)模型.

Bartolini等[1,3]提出了一种基于ABAC模型的访问控制策略模板,并在此基础上进一步使用用户故事(user stories)的概念来抽取出用户的隐私需求. 在他们的工作中,"同意"被视为策略的上下文属性. Drozdowicz等[4]给出基于ABAC模型的隐私策略本体语义,但其中缺乏对同意的形式描述及其在访问控制策略中的表示.

Ni和Bertino等人基于RBAC模型提出了一个支持授权和管理隐私感知(privacy-aware)访问控制策略的综合框架[5],其中增加了表示隐私相关的附加组件. 但Ni等以及其他相关研究[6,7]只是从目的限制的角度解决隐私数据访问控制,没有考虑用户的参与. Peyrone等人[8]从GDPR合规性的角度基于RBAC模型和Event-B语言设计出基于同意的隐私保护访问控制模型;其中将同意表示为一个静态的标签,不关注同意是如何授予、如何判断的,只关注同意应该如何管理,例如添加、删除、更新同意;对同意的控制缺乏有效的机制.

根据PDP的要求,访问控制系统应当允许个人完全控制他们的数据. 显然在上述文献中,当数据收集者收集了用户的个人数据之后,用户没有权限决定谁可以访问并处理他们的个人数据. 因此这些研究只能从数据收集者的角度讨论隐私保护,与PDP的要求有一定的差距,无法体现用户的自主可控.

除了上述研究之外,当前还有很多新的研究将区块链技术引入到隐私保护访问控制机制中[9,10]. 然而这些研究同样没有将数据主体的同意与访问控制技术有效的融合起来.

综上,现有隐私数据访问控制方法并不能满足PDP法规对隐私保护技术的需求. 我们需要设计一种由用户来授予的特殊权限,该类权限的授予和撤销都由用户来控制,以实现用户的自主可控. 为此,本文提出一种基于用户同意的隐私保护访问控制模型以及隐私保护协议,把目的限制、用户的"同意"作为隐私授权的基本要素. 本文的方法不但可以满足PDP法规的要求,还能提高用户的数据隐私保护性,通过实验表明该方案可以保证访问控制的安全性.

2　隐私保护访问控制分析与模型定义

2.1　隐私保护访问控制分析

虽然隐私数据也属于一种数据资源,但其访问控制机制与传统的访问控制机制相比,有其自身的特性:

(1)用户应参与隐私数据访问的决策,这样做一方面体现了用户的自主可控性,另一方面可以使用户能够接受更加灵活的访问方式来缓解隐私数据共享与隐私保护之间的矛盾[11];

(2)隐私数据的访问权限不能仅基于角色、属性等进行判断,而应该基于访问目的以及数据类别约束[12,13]、角色约束等更复杂的规则进行判断,以满足目的限制原则[14,15]和数据最小化原则[14~16];

(3)与传统访问控制模型不同,隐私数据的访问控制没有角色层次的概念,所有的角色都为私有角色,权限不能被继承,因此权限也都是私有权限,这样可以避免隐私泄露;

(4)对个人数据的访问控制除了需要考虑管理授权(或称资源访问授权)之外,还应考虑一类特殊的授权——隐私授权,本文也称为同意授权. 根据数据主体(即用户)的隐私要求(即在数据收集的时候与数据收集者达成的协议)来进行同意授权,决定是否同意或拒绝;管理授权则是在获得同意授权之后,由数据控制者、数据处理者和第三方共同来参与的一般数据处理授权行为,属于传统的授权. 因此,隐私保护访问控制是一种双重的访问控制. 我们后面把经同意授权的权限称为同意权限.

2.2　隐私保护访问控制模型

为了避免数据主体逐个地去授予同意或者访问请求者逐一去向数据主体申请同意,本文按照数据的类型来收集个人数据[6],并且将数据主体对某类个人数据集的相同保护要求进行抽取,统一管理. 本文设计了三种管理器:同意决策器(Consent Decider,CD)、授权决策器(Authorization Decider, AD)和访问控制器(Access Controler,AC). 其中CD被视为数据主体的代理,由其判断是否同意、授权同意权限. AD根据请求者在隐私保护模型中的角色来判断请求者是否有基础访问权限. 这样,只有请求者获得同意权限和基础访问权限之后,才获得数据的访问权限. AC根据CD和AD的结果来完成访问请求的判断. 如果CD撤销同意,则AC随时可以拒绝访问者. 隐私保护访问控制流程如图1所示.

CD、AD和AC的管理类动作定义如下:

$$a::=a_{\mathrm{CD}}|a_{\mathrm{AD}}|a_{\mathrm{AC}}|a_1;\ a_2 \tag{1}$$

$$a_{\mathrm{CD}}::=a_{\mathrm{con}}|a_{\mathrm{denyCon}}|a_{\mathrm{revCon}} \tag{2}$$

$$a_{\mathrm{AD}}::=a_{\mathrm{deny}}|a_{\mathrm{auth}} \tag{3}$$

$$a_{\mathrm{AC}}::=a_{\mathrm{reject}}|a_{\mathrm{accept}}|a_u \tag{4}$$

其中,式(1)中的a_{CD}、a_{AD}和a_{AC}分别表示CD、AD和AC的原子管理动作,a_1;a_2表示复合动作,为动作的顺序执行;式(2)中a_{con}、a_{denyCon}和a_{revCon}分别表示同意、拒绝同意和撤销同意动作;式(3)中a_{deny}和a_{auth}分别表示否认和授权动作;式(4)中a_{reject}、a_{accept}和a_u分别表示拒绝请求、接受请求和用户u的角色判断.

后面用集合A_{act}表示所有管理类动作的集合,即$A_{\mathrm{act}}=\{a_u,a_{\mathrm{con}},a_{\mathrm{denyCon}},a_{\mathrm{reject}},a_{\mathrm{revCon}},a_{\mathrm{deny}},a_{\mathrm{auth}},a_{\mathrm{accept}}\}$.

本文综合参考了三种RBAC模型:RBAC96模

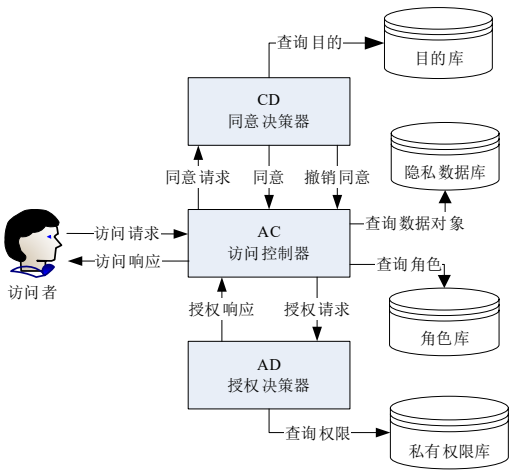


图1 隐私保护访问控制流程

型[17]、ARBAC97(Administrative RBAC'97)模型[18]和NIST(National Institute of Standards and Technology)RBAC模型[19],提出隐私保护模型.结合图1及Truong等[20]描述的一个实际场景抽取出四类私有角色:数据主体(Data Subject,DS)、数据收集者(Data Collector,DC)、数据处理者(Data Processor,DP)和第三方(Third Party,TP).根据PDP的要求[14,15]给出隐私保护的访问控制PPAC(Privacy Preserving Access Control)模型.

PPAC模型定义如式(5)所示:

$$(R_{\mathrm{P}},R_{\mathrm{A}},D,E,Q,\mathrm{can}_{\mathrm{A}},\mathrm{can}_{\mathrm{B}},\mathrm{can}_{\mathrm{C}},W,G) \tag{5}$$

其中,$R_{\mathrm{P}}=\{r_{\mathrm{DS}},r_{\mathrm{DC}},r_{\mathrm{DP}},r_{\mathrm{TP}}\}$为私有角色集合,其中下标P表示私有(private);$R_{\mathrm{A}}=\{r_{\mathrm{CD}},r_{\mathrm{AD}},r_{\mathrm{AC}}\}$为管理角色集合,其中下标A表示管理(administrative);D为个人数据类别集合,其中$d\in D$为某一类个人数据的标识符;E表示目的集合,其中包括了收集目的集合C,即$C\subseteq E$;$Q\subseteq U\times O\times D\times E$为访问请求集合,其中$U$为用户集合,$O$为数据操作集合,包含了collect,record,delete,read和write等基本数据操作;用$q=(u,o,d,e)\in Q$表示一个访问请求个体;$\mathrm{can}_{\mathrm{A}}$:$R_{\mathrm{A}}\times A_{\mathrm{act}}\to P_{\mathrm{A}}$表示从管理角色和管理动作的二元组到管理权限集合的映射,其中,P_{A}为管理权限集合,对$r\in R_{\mathrm{A}}$,$a\in A_{\mathrm{act}}$,$\mathrm{can}_{\mathrm{A}}(r,a)$表示管理角色$r$可以执行$a$动作,令$p_{\mathrm{A}}=\mathrm{can}_{\mathrm{A}}(r,a)$,则有$p_{\mathrm{A}}\in P_{\mathrm{A}}$;$\mathrm{can}_{\mathrm{B}}$:$O\times D\to P_{\mathrm{B}}$表示从操作和数据的二元组到基础权限集合的映射,其中P_{B}为基础访问权限集合,下标B表示基础(basic),若$\exists p_{\mathrm{B}}\in P_{\mathrm{B}}$且$\mathrm{can}_{\mathrm{B}}(o,d)=p_{\mathrm{B}}$,则表示AD授权对$d$执行$o$操作;$\mathrm{can}_{\mathrm{C}}$:$U\times O\times D\to P_{\mathrm{C}}$表示从用户、操作和数据三元组到同意权限集合的映射,其中P_{C}为同意权限集合,下标C表示同意(consent),对$u\in U$,$o\in O$,$d\in D$,若$\exists p_{\mathrm{C}}\in P_{\mathrm{C}}$且$\mathrm{can}_{\mathrm{C}}(u,o,d)=p_{\mathrm{C}}$,则表示CD同意$u$对$d$执行$o$操作;$W\subseteq U\times D$,对$u\in U$,$d\in D$,$(u,d)\in W$表示用户$u$为$d$的数据主体;$G\subseteq U\times U$,对$u_1$、$u_2\in U$,$(u_1,u_2)\in G$表示$u_1$是$u_2$的代理.

PPAC模型只列出了增加或含义发生变化的元素及关系,未出现的符号包含于RBAC模型中.

3 基于用户同意的隐私保护协议

3.1 协议的语法规则

CD进行同意授权通常基于某个特殊目的[21].本文参考文献[22],将目的合规性定义如下:

对$d\in D$,令$e\in E$为d的访问目的,C为d的收集目的集合,称e合规于C,当且仅当$e\in C$,记为complie(e,C).

给定PPAC模型,访问控制公式φ定义如式(6):

$$\begin{aligned}\varphi::=&\ \mathrm{UA}(u,r)|\mathrm{PA}(p,r)|\mathrm{owner}(u,d)|\mathrm{user}(u)\\&|\mathrm{complie}(e,C)|\mathrm{delegate}(u_1,u_2)\\&|\mathrm{accept}(q)|\mathrm{reject}(q)|\mathrm{con}(q)|\mathrm{auth}(q)\\&|\mathrm{denyCon}(q)|\mathrm{deny}(q)|\mathrm{revCon}(q)\\&|[a]\varphi|\Box\varphi|\Diamond\varphi|\neg\varphi|\varphi_1\wedge\varphi_2|\varphi_1\to\varphi_2\end{aligned} \tag{6}$$

其中,UA(u,r)表示u的角色为r;PA(p,r)表示角色r有基础访问权限p;owner(u,d)表示$(u,d)\in W$;user(u)表示u为用户;complie(e,C)表示e与C合规;delegate(u_1,u_2)表示$(u_1,u_2)\in G$;accept(q)和reject(q)分别表示q被接受和拒绝;con(q)、denyCon(q)和revCon(q)分别表示同意、拒绝同意和撤销同意q;auth(q)和deny(q)分别表示对q授权和否认授权;[a]表示动作a的执行,[]为动作算子;$\Box\varphi$表示"未来任意时刻"φ,$\Diamond\varphi$表示"未来某一时刻"φ.由φ组成的集合用Φ表示.含时态算子$\Box$、$\Diamond$的公式称为时序公式,含[]动作算子的公式称为动作公式,其他的为状态公式.

给定PPAC模型,对$q=(u,o,d,e)\in Q$,$C\subseteq E$,基于用户同意的隐私保护协议包含动作规则集合Ψ,如表1所示.其中,Rule1~Rule5表示AC的动作规则,Rule6~Rule11表示CD的动作规则(本文省略了对p_{C}的添加和删除规则),Rule12~Rule14表示AD的动作规则,Rule15为复合动作规则.其中$\exists p_{\mathrm{B}}\in P_{\mathrm{B}}$:$\mathrm{can}_{\mathrm{B}}(o,d)=p_{\mathrm{B}}$表示对基础权限进行查询.

3.2 协议的语义模型

PPAC协议的语义模型定义为一个迁移系统,如式(7)所示:

$$M=(S,S_0,A_d,\sigma,\Theta,V,F) \tag{7}$$

其中,S表示状态集合,$S=S_{\mathrm{AC}}\times S_{\mathrm{CD}}\times S_{\mathrm{AD}}$,其中,$S_{\mathrm{AC}}=\{\mathrm{requesting},\mathrm{consented},\mathrm{accepted},\mathrm{rejected}\}$,$S_{\mathrm{CD}}=\{\mathrm{waiting},\mathrm{consent},\mathrm{denyConsent},\mathrm{revokeConsent}\}$;$S_{\mathrm{AD}}=\{\mathrm{waiting},\mathrm{authorize},\mathrm{deny}\}$;$S_0$表示初始状态集合,$S_0=S_{\mathrm{AC}_0}\times S_{\mathrm{CD}_0}\times S_{\mathrm{AD}_0}$,其中,$S_{\mathrm{AC}_0}=\{\mathrm{requesting}\}$,$S_{\mathrm{CD}_0}=S_{\mathrm{AD}_0}=\{\mathrm{waiting}\}$;$A_d$为管理动作集合;$\sigma$:$S\times A_{\mathrm{act}}\to S$表示权限状态的迁移,对

表1　动作规则集合 Ψ

规则	逻辑表示
Rule1	$[a_u](\text{owner}(u,d)\wedge\text{user}(u))\rightarrow\text{UA}(u,r_{\text{DS}})$
Rule2	$[a_u](\text{user}(u)\wedge(\exists u'\in U{:}\text{delegate}(u,u')\wedge\text{UA}(u',r_{\text{DC}})))\rightarrow\text{UA}(u,r_{\text{DP}})$
Rule3	$[a_u](\text{user}(u)\wedge\neg(\text{UA}(u,r_{\text{DS}})\wedge\text{UA}(u,r_{\text{DP}})\wedge\text{UA}(u,r_{\text{DC}})))\rightarrow\text{UA}(u,r_{\text{TP}})$
Rule4	$[a_{\text{accept}}](\text{con}(q)\wedge\text{auth}(q))\rightarrow\text{accept}(q)$
Rule5	$[a_{\text{reject}}](\text{denyCon}(q)\vee\text{revCon}(q)\vee\text{deny}(q))\rightarrow\text{reject}(q)$
Rule6	$[a_{\text{con}}]\text{UA}(u,r_{\text{DS}})\rightarrow\text{con}(q)$
Rule7	$[a_{\text{con}}](\text{complie}(e,C)\wedge\text{UA}(u,r_{\text{DC}}))\rightarrow\text{con}(q)$
Rule8	$[a_{\text{con}}](\text{complie}(e,C)\wedge\text{UA}(u,r_{\text{DP}})\wedge(\exists u'\in U{:}\text{delegate}(u,u')\wedge\text{con}(q')))\rightarrow\text{con}(q)$, 其中, $q'=(u',o,d,e)$
Rule9	$[a_{\text{con}}](\text{complie}(e,C)\wedge\text{UA}(u,r_{\text{TP}}))\rightarrow\text{con}(q)$
Rule10	$[a_{\text{denyCon}}](\neg\text{complie}(e,C)\wedge\neg\text{UA}(u,r_{\text{DS}}))\rightarrow\text{denyCon}(q)$
Rule11	$[a_{\text{revCon}}](\neg\text{complie}(e,C)\wedge\text{con}(q))\rightarrow\text{revCon}(q)$
Rule12	$[a_{\text{auth}}](\exists p_{\text{B}}\in P_{\text{B}}{:}(\text{can}_{\text{B}}(o,d)=p_{\text{B}})\wedge\text{PA}(p_{\text{B}},r_{\text{TP}})\wedge\text{UA}(u,r_{\text{TP}}))\rightarrow\text{auth}(q)$
Rule13	$[a_{\text{deny}}](\nexists p_{\text{B}}\in P_{\text{B}}{:}\text{can}_{\text{B}}(o,d)=p_{\text{B}}\wedge\text{PA}(p_{\text{B}},r_{\text{TP}})\wedge\text{UA}(u,r_{\text{TP}}))\rightarrow\text{deny}(q)$
Rule14	$[a_{\text{auth}}](\text{UA}(u,r_{\text{DC}})\vee\text{UA}(u,r_{\text{DS}})\vee\text{UA}(u,r_{\text{DP}}))\rightarrow\text{auth}(q)$
Rule15	$[a_1;a_2]\varphi\rightarrow[a_2]([a_1]\varphi)$

动作 $a\in A_{\text{act}}$, $s,s'\in S$, 则 $\sigma(s,a)=s'$ 表示执行动作 a 后状态 s 变为 s', 也表示为 $s\xrightarrow{a}s'$; $\Theta\subseteq P_{\text{A}}\times\Psi\times R_{\text{A}}$ 为状态迁移规则, 也称为授权策略. 给定 $\theta=(p_{\text{A}},\psi,r)\in\Theta$, 则 $s\rightarrow_{\theta}s'$ 表示从状态 s 到 s' 一步迁移是 θ 允许的, $s\xrightarrow{*}_{\theta}s'$ 表示从 s 到 s' 存在0步或多步状态迁移序列是 θ 允许的, 或称 s' 是从 s 开始 θ 可达的, 简称 s' 是可达的; $V{:}S\times\Phi\rightarrow\{\text{true},\text{false}\}$ 为赋值函数, 对一个给定状态 s 中的 $\varphi\in\Phi$ 指派真值: 当 φ 为状态公式时, 若 φ 在 s 中解释为 true, 即 $V(s,\varphi)=\text{true}$, 则记作 $s\vDash\varphi$; 当 φ 为时序公式时, 对状态序列 $s_0,\cdots,s_i,\cdots,s_j,\cdots$, 假设 $\varphi=\Box\varphi'$, 则 $s_i\vDash\Box\varphi'$ 当且仅当对 $\forall s_j(j\geqslant i)$ 都有 $s_j\vDash\varphi'$; 假设 $\varphi=\Diamond\varphi'$, 则 $s_i\vDash\Diamond\varphi'$ 当且仅当 $\exists s_j(j\geqslant i)$ 满足 $s_j\vDash\varphi'$; 当 $\varphi=[a]\varphi'$ 时, 其中 a 为管理类动作, 则 $s_i\vDash[a]\varphi'$ 当且仅当 $\exists s_j(j\geqslant i)$, $s_j\vDash\varphi''$ 且 $[a]\varphi'\rightarrow\varphi''\in\Psi$, 其中 φ' 和 φ'' 均为状态公式; $F\subseteq S$ 表示终止状态, 也称为可接受状态集合, 只要 AC 处于 accepted 和 rejected 状态之一, 就表示迁移系统到达了可接受状态.

当模型 M 在状态 s 下满足式 φ 时, 记为 $M,s\vDash\varphi$.

整个语义模型是由 AC、CD 和 AD 三个状态自动机组合成的一个自动机网络, 其中, 每个状态自动机的迁移图如图2所示, 其中, 循环箭头表示当其他动作发生时该状态没有改变.

3.3　安全性定义和分析

我们给出一个授权实例测试定义, 从而进一步定义协议的安全性.

给定 PPAC 协议的语义模型 M, 一个授权实例测试表示为 $<s,q,\Theta>$. 如果存在状态 s' 满足 $s\xrightarrow{*}_{\Theta}s'$ 且 $M,s'\vDash\text{accept}(q)$, 则称 q 在 s 和 Θ 下是可接受的(或可授权的), 记为 $s\vdash_{\Theta}q$; 如果存在 s' 满足 $s\xrightarrow{*}_{\Theta}s'$ 且 $M,s'\vDash\text{reject}(q)$, 则称 q 在 s 和 Θ 下是拒绝的(或不可授权的), 记为 $s\nvdash_{\Theta}q$.

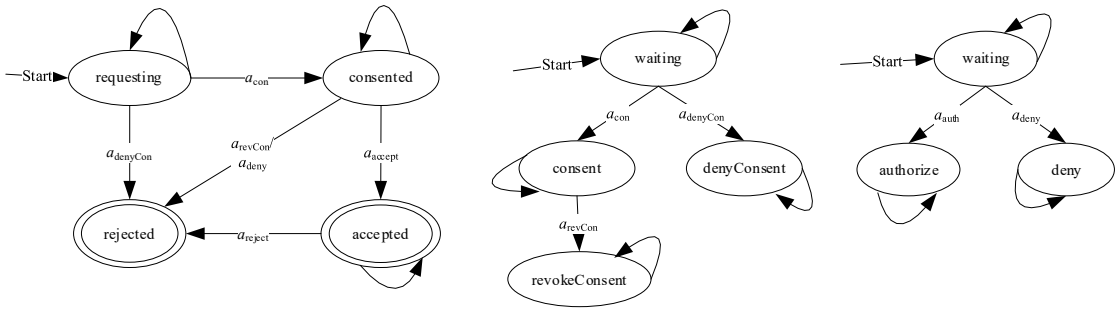
安全性定义如下:

给定 PPAC 协议的语义模型 $M=(S,S_0,A_d,\sigma,\Theta,V,F)$, 如果从 $s_0\in S_0$ 出发, 根据迁移规则 Θ, 对 $q=(u,o,d,e)$ 的测试行为最终都能到达终止状态(rejected 或 accepted), 即存在有限的迁移动作序列 $a_1,\cdots,a_i,\cdots,a_m(a_i\in A_d,1\leqslant i\leqslant m)$ 及状态序列 $s_0,s_1,\cdots,s_k,\cdots$, $\exists s_n(n\geqslant 0)$ 满足 $s_0\xrightarrow{a_1,a_2,\cdots,a_m}_{\Theta}s_n$ 且 $s_n\vdash_{\Theta}q$ 或 $s_n\nvdash_{\Theta}q$ 则称该模型的执行是隐私保护访问控制安全的.

给定语义模型 M, 对请求 q, 我们将安全性分解为如下三类性质:

(1)双重授权性质: 如果同意该请求, 且该访问者获得了访问授权, 则该请求会被接受, 即

$$M\vDash\Box(\text{con}(q)\wedge\text{auth}(q)\rightarrow\Diamond\text{accept}(q)) \tag{8}$$



(a) AC 自动机　　(b) CD 自动机　　(c) AD 自动机

图2　三个状态自动机迁移图

(2)撤销同意性质:在该请求获得同意后,如果数据主体撤销同意,则最终该请求被拒绝,即

$$M\models\Box(\text{revCon}(q)\rightarrow\Diamond\Box\text{reject}(q)) \tag{9}$$

(3)拒绝性质:如果拒绝同意或否认授权,则最终该请求被拒绝,即

$$M\models\Box(\text{denyCon}(q)\vee\text{deny}(q)\rightarrow\Diamond\Box\text{reject}(q)) \tag{10}$$

上述性质证明过程如下:

(1)双重授权性质证明

证明

若证式(8),即证对任意的状态序列$s_0,\cdots,s_i,\cdots,s_j,\cdots$和迁移规则集合$\Theta$,当$\exists s_j(j\geqslant 0)$满足$s_0\xrightarrow{*}_{\Theta}s_j$,使得$M,s_j\models\text{con}(q)\wedge\text{auth}(q)$时,有$M,s_j\models\Diamond\text{accept}(q)$成立.

当$M,s_j\models\text{con}(q)\wedge\text{auth}(q)$成立时,有$s_j\models\text{con}(q)$且$s_j\models\text{auth}(q)$,由此可知complie$(e,C)$成立,则对用户$u$,

(a)当已知u为DC用户,即UA(u,r_{DC})成立时,根据Rule7和Rule14,$\exists s_m,s_n(0\leqslant m<n\leqslant j)$和动作$a_{\text{con}}$、$a_{\text{auth}}$使得$s_0\xrightarrow{a_{\text{con}}}_{\Theta}s_m\rightarrow\cdots\rightarrow s_n\xrightarrow{a_{\text{auth}}}_{\Theta}s_j$,且$s_m\models\text{con}(q)$,$s_j\models\text{con}(q)\wedge\text{auth}(q)$. 根据Rule4,存在动作$a_{\text{accept}}$及状态$s_h,s_k(j\leqslant h\leqslant k)$满足$s_j\rightarrow\cdots\rightarrow s_h\xrightarrow{a_{\text{accept}}}_{\Theta}s_k$,且$s_k\models\text{accept}(q)$,则对状态$s_j$,当$s_j\models\text{con}(q)\wedge\text{auth}(q)$成立时,有$M,s_j\models\Diamond\text{accept}(q)$成立.

(b)当u不是DC用户时,根据Rule1~Rule3对u的角色进行判断,执行a_u动作,即$\exists s_i(0\leqslant i\leqslant j)$满足$s_0\xrightarrow{a_u}_{\Theta}s_i$且$s_i\models\text{UA}(u,r_{\text{DS}})$或$s_i\models\text{UA}(u,r_{\text{DP}})$或$s_i\models\text{UA}(u,r_{\text{TP}})$,与(1)同理,根据Rule6、Rule8、Rule9及Rule4,可证$M,s_j\models\Diamond\text{accept}(q)$成立.

因此,对任意的状态序列$s_0,\cdots,s_i,\cdots,s_j,\cdots$,从状态$s_0$出发,存在动作序列$a_{\text{con}},a_{\text{auth}},a_{\text{accept}}$(或$a_u,a_{\text{con}},a_{\text{auth}},a_{\text{accept}}$)和迁移规则$\theta\in\Theta$,使得$M\models\Box(\text{con}(q)\wedge\text{auth}(q)\rightarrow\Diamond\text{accept}(q))$成立. 性质(1)成立.

证毕.

(2)撤销同意性质证明

证明

若证式(9),即证对任意的状态序列$s_0,\cdots,s_i,\cdots,s_j,\cdots$,对迁移规则集合$\Theta$,当$\exists s_j(j\geqslant 0)$满足$s_0\xrightarrow{*}_{\Theta}s_j$,使得$M,s_j\models\text{revCon}(q)$时有$M,s_j\models\Diamond\Box\text{reject}(q)$成立.

与性质(1)的证明过程类似,当$M,s_j\models\text{revCon}(q)$时,有$s_j\models\text{revCon}(q)$,根据Rule11,存在状态$s_i(0<i<j)$满足$s_i\models\neg\text{complie}(e,C)\wedge\text{con}(q)$且$s_i\xrightarrow{a_{\text{revCon}}}_{\Theta}s_j$.

(a)当UA(u,r_{DC})成立时,根据Rule7,$\exists s_m,s_n(0\leqslant m<n<i)$和动作$a_{\text{con}}$使得$s_0\rightarrow\cdots\rightarrow s_m\xrightarrow{a_{\text{con}}}_{\Theta}s_n\rightarrow\cdots\rightarrow s_i$,其中$s_m\models\text{complie}(e,C)$,$s_n\models\text{con}(q)$. 将断言complie$(e,C)$变成$\neg$complie$(e,C)$的动作不在本文的讨论范围内,这里假设存在该类动作,执行后使得$s_i\models\neg\text{complie}(e,C)$成立. 因此,根据Rule11,存在动作$a_{\text{revCon}}$,使得$s_i\xrightarrow{a_{\text{revCon}}}_{\Theta}s_j$成立且$s_j\models\text{revCon}(q)$. 根据Rule5,存在动作$a_{\text{reject}}$及状态$s_h,s_k(j\leqslant h<k)$满足$s_j\rightarrow\cdots\rightarrow s_h\xrightarrow{a_{\text{reject}}}_{\Theta}s_k$,且$s_h\models\text{revCon}(q)$及$s_k\models\text{reject}(q)$,因此对状态$s_j$,当$s_j\models\text{revCon}(q)$成立时,有$M,s_j\models\Diamond\text{reject}(q)$成立. 对$\forall s_x(j<k\leqslant x)$,没有任何规则修改reject$(q)$,即$s_x\models\text{reject}(q)$,因此$M,s_j\models\Diamond\Box\text{reject}(q)$成立.

(b)当u不是DC用户时,执行a_u动作,根据Rule1~Rule3对u的角色进行判断,即$\exists s_f(0\leqslant f<i)$满足$s_0\rightarrow\cdots\xrightarrow{a_u}_{\Theta}s_f$,$s_f\models\text{UA}(u,r_{\text{DS}})\vee\text{UA}(u,r_{\text{DP}})\vee\text{UA}(u,r_{\text{TP}})$,与(1)同理,根据Rule6、Rule8和Rule9可知$\exists s_m(f<m<i)$和动作a_{con},使得$s_f\rightarrow\cdots\xrightarrow{a_{\text{con}}}_{\Theta}s_m\rightarrow\cdots\rightarrow s_i$,其中,$s_m\models\text{con}(q)$,$s_i\models\neg\text{complie}(e,C)\wedge\text{con}(q)$. 根据Rule11,存在动作$a_{\text{revCon}}$满足$s_i\xrightarrow{a_{\text{revCon}}}_{\Theta}s_j$且$s_j\models\text{revCon}(q)$. 根据Rule5,存在动作$a_{\text{reject}}$及状态$s_h,s_k(j\leqslant h<k)$满足$s_j\rightarrow\cdots\rightarrow s_h\xrightarrow{a_{\text{reject}}}_{\Theta}s_k$,且$s_h\models\text{revCon}(q)$及$s_k\models\text{reject}(q)$,因此,对状态$s_j$,当$s_j\models\text{revCon}(q)$成立时,有$M,s_j\models\Diamond\text{reject}(q)$成立. 同($a$),有$M,s_j\models\Diamond\Box\text{reject}(q)$成立.

因此,对任意的状态序列$s_0,\cdots,s_i,\cdots,s_j,\cdots$,从状态$s_0$出发,存在动作序列$a_{\text{con}},a_{\text{revCon}},a_{\text{reject}}$(或$a_u,a_{\text{con}},a_{\text{revCon}},a_{\text{reject}}$)和迁移规则$\theta\in\Theta$,使得$M\models\Box(\text{revCon}(q)\rightarrow\Diamond\Box\text{reject}(q))$成立. 性质(2)成立.

证毕.

(3)拒绝性质的证明类似于(2),这里省略. 证毕.

4 实验评估和比较

为了验证协议的安全性,本文用TLA+(Temporal Logic of Actions plus)语言(一种描述并发与分布式系统的形式化规约语言)表示隐私保护协议,并通过TLC模型检测器(一种用于查找TLA+规约中错误的程序)来自动验证这些性质是否满足. TLA+语法和含义具体内容可以参见文献[23].

实验环境为:Windows 10系统,12th Gen Intel Core i7-12700,DDR4 3 200 MHz 32 GB,TLA+1.7.1版本.

由于变量规模较大,容易产生状态爆炸. 为了遍历所有验证路径,本文采用两种最小模型的验证方法,一种按照角色的分类设置最小模型进行验证,包括DP-DC模型、DS模型、TP模型;另一种将四类角色同时包

括进行最小模型进行验证,即four-roles模型.本文参考文献[24]的做法,当不同状态的数量超过1 000万时,人工停止测试.

4.1 实验评估

在相同角色所对应的用户集合下,将(|C|,|E|)作为一个模型的数据集.根据实验数据,图3显示了不同模型的实验结果中每秒探测的状态数与数据的规模(取|C|/|E|)之间的关系.

本实验验证的系统规约如式(11)所示,为TLA+的系统规约一般表达式:

$$ACSpec \triangleq ACInit \wedge \Box[ACNext]_{vars} \wedge Properties \quad (11)$$

其中,ACSpec表示访问控制系统规约或说明,ACInit表示初始状态,ACNext表示后继状态动作,vars表示所有变量的组合,Properties表示所有性质的合取式.利用TLC工具检测所有后续状态是否满足性质,如果不满足,则会提示反例.尽管验证的状态有限,本实验的结果仍然含有正常结束的情况,未来模型还有进一步优化的空间.所有的实验都未出现反例,因此,本协议满足安全性.

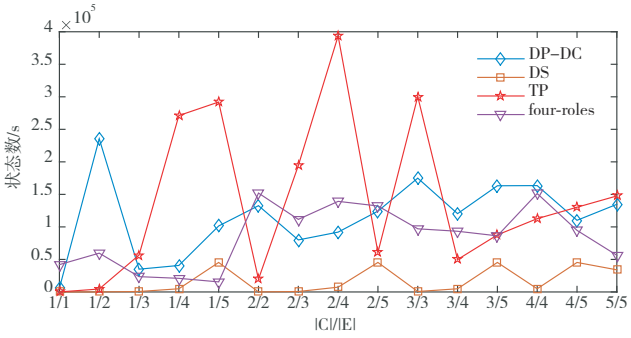


图3　最小模型测试每秒状态数和数据规模关系图

4.2 与现有相关工作对比

本节从形式化表示的角度对比不同的模型对GDPR中的条款是否有对应的描述,从而详细说明本文与其他研究的不同及优势,如表2所示.

从表2比较可以看出,已有的研究并没有出现"同意权限"的概念及其形式化表示.

表2　本文研究与其他研究在隐私保护条款上是否有对应表示的对比

序号	具体内容	文献[1]	文献[3]	文献[4]	文献[5]	文献[6]	文献[7]	文献[8]	文献[9]	文献[10]	本文
1	DC决定个人数据处理的目的和方式	√			√	√	√		√		√
2	DP是代表DC处理个人数据的实体				√				√		√
3	TP指除了DS、DC、DP之外的机构或组织										√
4	个人数据的处理必须是合法的、明确的,并忠实于DS	√	√		√				√		√
5	个人数据的收集和处理必须具备特殊的目的	√	√	√	√	√	√		√	√	√
6	个人数据的收集必须基于DS的同意	√			√				√		√
7	DS需要在处理个人数据之前签署同意	√	√					√	√		√
8	DS有权随时撤销其同意		√					√	√		√
9	DS有对自己数据的处理权	√							√		√
10	DS有权从控制者那里得知其个人数据正在被处理的目的	√	√						√		√
11	DP必须经过DC的授权才可以处理个人数据;DC和DP不是一个角色				√				√		√
12	DS可以拒绝同意,DC根据DS拒绝同意而拒绝授权										√

5 结束语

文章分析了传统访问控制解决隐私保护问题存在的不足,引入了同意权限以满足用户对个人数据的自主可控需求.虽然提出的方法是以用户为中心的隐私保护,但该方法仍然满足了企业的隐私保护需求,因此该方法适用于解决目前任何场景的隐私保护要求,可以为组织机构的隐私保护合规性设计提供参考.后续工作还需要对同意权限进入深入分析,以获得更加灵活的授权机制.

参考文献

[1] BARTOLINI C, DAOUDAGH S, LENZINI G, et al. Towards a lawful authorized access: A preliminary GDPR-based authorized access[C]//Proceedings of the 14th Inter-

national Conference on Software Technologies. Setubal: SciTePress, 2019: 331-338.

[2] DAOUDAGH S, MARCHETTI E, SAVARINO V, et al. How to improve the GDPR compliance through consent management and access control[C]//Proceedings of the 7th International Conference on Information Systems Security and Privacy. Setubal:SciTePress, 2021: 534-541.

[3] BARTOLINI C, DAOUDAGH S, LENZINI G, et al. GDPR-based user stories in the access control perspective [M]//Communications in Computer and Information Science. Cham: Springer International Publishing, 2019: 3-17.

[4] DROZDOWICZ M, GANZHA M, PAPRZYCKI M. Semantic access control for privacy management of personal sensing in smart cities[J]. IEEE Transactions on Emerging Topics in Computing, 2022, 10(1): 199-210.

[5] NI Q, BERTINO E, LOBO J, et al. Privacy-aware role-based access control[J]. ACM Transactions on Information and System Security, 2010, 13(3): 1-31.

[6] WANG H A, CAO J L, ZHANG Y C. Building access control policy model for privacy preserving and testing policy conflicting problems[M]//Access Control Management in Cloud Environments. Cham: Springer International Publishing, 2020: 225-247.

[7] BYUN J W, LI N H. Purpose based access control for privacy protection in relational database systems[J]. The VLDB Journal, 2008, 17(4): 603-619.

[8] PEYRONE N, WICHADAKUL D. Formal models for consent-based privacy[J]. Journal of Logical and Algebraic Methods in Programming, 2022, 128: 100789.

[9] DAVARI M, BERTINO E. Access control model extensions to support data privacy protection based on GDPR [C]//2019 IEEE International Conference on Big Data (Big Data). Piscataway: IEEE, 2020: 4017-4024.

[10] WU G J, WANG S P, NING Z L, et al. Blockchain-enabled privacy-preserving access control for data publishing and sharing in the Internet of medical things[J]. IEEE Internet of Things Journal, 2022, 9(11): 8091-8104.

[11] KABIR M E, WANG H. Conditional purpose based access control model for privacy protection[C]//Proceedings of the Twentieth Australasian Conference on Australasian Database - Volume 92. New York: ACM, 2009: 135-142.

[12] COLOMBO P, FERRARI E. Efficient enforcement of action-aware purpose-based access control within relational database management systems[J]. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(8): 2134-2147.

[13] MAJEED A, LEE S. Anonymization techniques for privacy preserving data publishing: A comprehensive survey [J]. IEEE Access, 2020, 9: 8512-8545.

[14] VOIGT P, VON DEM BUSSCHE A. The EU General Data Protection Regulation (GDPR): A Practical Guide[M]. 1st Ed. Cham: Springer International Publishing, 2017.

[15] IT Governance Privacy Team, I T Governance. EU General Data Protection Regulation (GDPR) — An Implementation And Compliance Guide[M]. 4th edition. Ely: IT Governance Ltd, 2020.

[16] ČTVRTNÍK M. Data Minimisation—Storage limitation—archiving[M]//Archives and Records. Cham: Springer International Publishing, 2023: 197-240.

[17] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996, 29 (2): 38-47.

[18] SANDHU R, BHAMIDIPATI V, MUNAWER Q. The ARBAC97 model for role-based administration of roles [J]. ACM Transactions on Information and System Security, 1999, 2(1): 105-135.

[19] 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, 2001, 4(3): 224-274.

[20] TRUONG N B, SUN K, LEE G M, et al. GDPR-compliant personal data management: A blockchain-based solution[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 1746-1761.

[21] TOKAS S, OWE O. A formal framework for consent management[C]//Formal Techniques for Distributed Objects, Components, and Systems—FORTE 2020. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020: 169-186.

[22] COLOMBO P, FERRARI E. Enhancing MongoDB with purpose-based access control[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(6): 591-604.

[23] LAMPORT L, Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers[M]. Boston: Addison-Wesley Longman Publishing Co, Inc, 2002.

[24] 纪业, 魏恒峰, 黄宇, 等. CRDT 协议的 TLA+描述与验证[J]. 软件学报, 2020, 31(5): 1332-1352.
JI Y, WEI H F, HUANG Y, et al. Specifying and verify-

ing CRDT protocols using TLA+[J]. Journal of Software, 2020, 31(5): 1332-1352. (in Chinese)

作者简介

马　丽　女,1974年出生,安徽安庆人. 博士. 现为江西科技师范大学大数据科学学院讲师. 主要从事访问控制、隐私保护和形式化建模等方面的研究工作.
E-mail: mali@jxstnu.edu.cn

姜火文(通讯作者)　男,1974年出生,江西进贤人. 博士. 现为江西科技师范大学大数据科学学院教授、硕士生导师. 主要从事隐私保护、软件演化和计算机教育等方面的研究工作.
E-mail: jhw_604@163.com

彭　云　男,1972年出生,江西宜春人. 博士. 现为江西师范大学数字产业学院副教授、硕士生导师. 主要从事自然语言处理、人工智能与数据挖掘等方面的研究工作.
E-mail: pengyun@jxnu.edu.cn