

文章编号:1007-5321(2019)04-0121-05

DOI:10.13190/j.jbupt.2018-301

类型化隐式资源的隐私保护方法

段玉聪¹, 张友良², 白勇¹, 曹春杰¹

(1. 海南大学 信息科学与技术学院, 海南 海口 570228; 2. 海南大学 土木建筑工程学院, 海南 海口 570228)

摘要: 针对隐式隐私资源的建模和表述, 给出了一个基于元建模的对隐式资源概念进行语义界定的元模型概念体系, 解释了数据—信息—知识—智慧(DIKW)架构中的数据、信息、知识和智慧等基本类型化资源概念. 基于 DIKW 资源概念将现有知识图谱概念扩展为数据图谱、信息图谱和知识图谱, 进而提出了一种基于相同内容的不同资源表达处理效率差异和转换代价差异的可自动抽象调整的隐私保护解决架构. 根据要保护隐私目标的以计算代价衡量的保护程度, 制定将目标资源转换为何种类型资源. 通过对目标资源保护者的投入保护代价和攻击者的攻击代价的差异进行衡量, 选择最优的转换程度.

关键词: 隐式类型化资源; 隐私保护; 知识图谱; 数据—信息—知识—智慧架构

中图分类号: TP391.3

文献标志码: A

Privacy Protection Strategy for Implicit Typed Resources

DUAN Yu-cong¹, ZHANG You-liang², BAI Yong¹, CAO Chun-jie¹

(1. College of Information Science and Technology, Hainan University, Hainan Haikou 570228, China;

2. College of Civil Engineering and Architecture, Hainan University, Hainan Haikou 570228, China)

Abstract: Aiming at modeling and expressing of implicit privacy resources, a meta-model is proposed for semantic definition of implicit resource concepts. The meta-model explains the core concepts in data, information, knowledge wisdom (DIKW) architecture. Based on the DIKW resource concept, the existing knowledge map concept is extended to data graph, information graph and knowledge graph. An automatic abstract adjustment privacy protection solution is presented based on the difference of the processing efficiency of the same content expressed in different types of resources. Protection is specified as what types of resources to be converted and how much the conversions to be performed towards an optimal solution balancing the comprehensive value of both the investment of the protection side and the cost of attackers.

Key words: implicit typed resources; privacy protection; knowledge graph; data, information, knowledge wisdom architecture

随着边缘计算、大数据智能化的飞速发展以及物联网技术的普及和嵌入式设备的大量研发部署, 物联网中, 隐私保护研究的内容已经从对显式隐私内容^[1]进行保护扩展到了对隐式隐私内容^[2]进行保护. 本文基于对关系和实体存在意义上的探讨,

基于关系定义一切语义表达的背景, 在存在相关基础语义推理机制的基础上, 将对隐私模型表达概念体系构建起来后, 新观察到的数据语义完全由多维度的发生关联的其他类型的多层面关系所定义, 称之为类型化数据. 基于以前的工作^[3], 在一种三层

收稿日期: 2018-11-29

基金项目: 国家自然科学基金项目(61363007, 61662021); 赛尔网络下一代互联网创新项目(NGH20180607)

作者简介: 段玉聪(1977—), 男, 教授, 博士生导师, E-mail: duanyucong@hotmail.com.

可自动抽象调整的架构——数据—信息—知识—智慧架构 (DIKW, data, information, knowledge, wisdom) 图谱, 包括数据图谱、信息图谱和知识图谱的拓展, 将保护目标内容资源对应到 DIKW 隐私保护架构中的数据、信息和知识的类型化资源. 保护目标隐私资源时, 基于价值导向的权衡, 借助类型化资源转换、存储和传输的代价差异, 构建基于发掘和保护代价不对称程度的隐私资源保护方案.

1 相关工作

通常可以从隐私性、数据准确性、延时和能量消耗这几个方面对隐私保护方法的性能进行评估. Hundepool 等^[4]提出从群体中做出有用的推论, 同时保护贡献数据的个人隐私. Pearson 和 Charlesworth^[5]提出根据程序和技术解决方案设计的隐私保护方法. 隐私架构保护方案应避免内容遭受不期待的二次使用^[6]. 知识图谱是一个具有属性的实体被通过关系链接而成的网状知识库^[7]. Chaim^[8]提出了数据、信息和知识的定义概念. 构成数据、信息、知识和智慧的层次模型通常以金字塔形式表示^[9]. Duan 等^[10]从数据、信息、知识和智慧的角度阐明了知识图谱的结构. Sowa 等^[11]提出在逻辑、哲学和计算基础上表示知识. 数据可能采用隐式形式^[12]表示为信息图谱中的一系列关系.

2 资源类型建模

2.1 DIKW 元模型体系

借用概念模式 (Schema)^[13], 这个原来用于表达通过逻辑推理和时间维度的具体化来认知对象/经验的术语, 来表达资源之间的概念关联. 基于前期提出的关系定义一切语义 (relationship defined everything of semantics)^[14-15]建模模型和存在计算 (existence computation)^[16]推理机制, 给出了类型化 DIKW 概念化模式体系. 核心元素包括整体性、实体和关系. 观察者通过观察得到, 或对内部结构化或非结构化资源的归类而得到数据. 通过抽象时态或者其他关联关系而形成抽象实体. 表达语义的关系被赋予概念体的整体性的独立存在意义从而被当为一个认识对象实体. 整体性的语义包括: 一致性和完整性. 而实体是整体性的概念继承子类. 一致性和完整性分别基于“相等”或者“相同”概念的逻辑判断和数量判断. 将概念化 (Conceptualization) 过程总结为 3 个部分: 抽象 (Abstraction)、一般化 (GL, generalization) 和演绎 (Deduction). 对应的概念化导

出了类型化的数据、信息和知识的类型化的模式表达: $\text{Data}_{\text{Typed}}$ 、 $\text{Information}_{\text{Typed}}$ 、 $\text{Knowledge}_{\text{Typed}}$.

$\text{Unity} ::= \langle \text{Semantic}_{\text{Consistency}}, \text{Semantic}_{\text{Completeness}} \rangle$

OR $\langle \text{Consistency}, \text{Completeness} \rangle$

$\text{Entity} ::= \text{GL}^- (\text{Unity})$

Conceptualization

$:: = \langle \text{Abstraction}, \text{Generalization}, \text{Reduction} \rangle$

$\text{Abstraction} ::= \text{Collect}(\text{shared}(\text{element}))$

$\text{Abstraction}_{\text{existing}}$

$:: = \text{Collect}_{\text{Bottom-Up}}(\text{shared}(\text{element}(\text{discrete}_{\text{Assumption}})))$

$\text{Abstraction}_{\text{TypedDIKW}}$

$:: = \text{Collect}_{\text{Networked}}(\text{shared}(\text{Type}_{\text{attribute}}, \text{Type}_{\text{method}}))$

将类型化 DIKW 概念体系扩展到元素, 称之为完全类型化元素. 例如新观察或认识到的数据的识别过程将完全基于已经被类型化的概念. 任何基于此体系的新概念的语义将完全由多维度的已存在的发生关联的其它类型的元素及关系所表述和定义.

$\text{Data}_{\text{Typed}}$

$:: = \text{Static}(\text{Abstraction}_{\text{TypedDIKW}}(\text{Type}_{\text{attribute}}, \text{Type}_{\text{method}}))$

类型化信息代表了依赖于类型化数据的存在而标记的被关联的多于一个的类型化数据. 类型化信息可以是标量等不具有独立存在性的内容.

$\text{Information}_{\text{Typed}}$

$:: = \text{Dynamic}(\text{Abstraction}_{\text{TypedDIKW}}(\text{Interaction}, \text{Usage})_{(\text{TypeAttribute}, \text{TypeMethod})})$

类型化知识指基于概率统计出的经验, 或者基于直接观察类型化资源或间接推理类型化资源中抽象出的类别推理.

$\text{Knowledge}_{\text{Typed}}$

$:: = \text{Induction}(\text{Abstraction}_{\text{TypedDIKW}}(\text{Data}_{\text{Typed}}, \text{AND Information}_{\text{Typed}}))$

借叔本华的直觉^[16], 取智慧作为推理和意志之间的平衡, 以优化人类的长期目标, 作为“智慧”.

2.2 类型化资源

定义 1 类型化资源 (TR_{DIKW} , typed resource)

$\text{TR}_{\text{DIKW}} ::= \langle D_{\text{DIKW}}, I_{\text{DIKW}}, K_{\text{DIKW}} \rangle$

TR_{DIKW} 包括数据 D_{DIKW} 、信息 I_{DIKW} 和知识 K_{DIKW} . D_{DIKW} 没有被特定的利益相关者或机器指定. D_{DIKW} 被赋予概念体的独立存在意义, 从而被当做一个认识对象实体数据, 或者可以通过抽象关系而形成抽象实体

数据,脱离被观察状态或者被观察背景的观察对象的存在认识的唯一性将基于“相等”或者“相同”概念的判断. I_{DIK} 代表人类直接或间接观察到或进行交互的 D_{DIK} 或 I_{DIK} . K_{DIK} 代表抽象的 D_{DIK} 、 I_{DIK} 和 K_{DIK} . K_{DIK} 基于概率统计出的经验,或者基于直接观察类型化资源或间接推理类型化资源中抽象出的类别推理. 利用 K_{DIK} 来推理和预测未知资源或未观察到的关系.

定义2 DIKWGraph

在三层数据图谱 DG_{DIK} , 信息图谱 IG_{DIK} 和知识图谱 KG_{DIK} 中拓展了常用的知识图谱的概念:

$\text{DIKWGraph}::=\langle (\text{DG}_{\text{DIK}}), (\text{IG}_{\text{DIK}}), (\text{KG}_{\text{DIK}}) \rangle$

定义3 DG_{DIK}

$\text{DG}_{\text{DIK}}::=\text{Structure}_{\text{frequency}} \{ \text{array}, \text{tree}, \text{graph} \}$

DG_{DIK} 可以记录实体的基本结构,是各种数据结构,即数组、链表、栈、树和图等集合. DIKW 架构借助从 DG_{DIK} 上以实体综合频度计算为核心的分析到 IG_{DIK} 和 KG_{DIK} 上的自适应的自动抽象的资源优化过程支持经验知识引入和高效自动语义分析. DG_{DIK} 记录 D_{DIK} 的频度, D_{DIK} 的频度包括使用频度 U 、关联频度 R 和变异频度 C . U 指使用 D_{DIK} 的总次数, R 指 D_{DIK} 与其他类型化资源之间的总关联数, C 指 D_{DIK} 的变化总次数. U 、 R 和 C 由3个基本频度构成,包括时间频度 M 、空间频度 I 和结构频度 S . I 为 D_{DIK} 的空间轨迹总数, S 为 D_{DIK} 在不同结构中出现的总次数. D_{DIK} 由综合频度 V 表示,不同的 D_{DIK} 具有不同的 V , V 由综合计算 U 、 R 和 C 的值得到,即 $D_{\text{DIK}} = V(U, R, C)$. U 、 R 和 C 的值由 M 、 I 和 S 的值综合计算得到. 计算 M 时,用 $i(x, y, z)$ 标注三维空间中一个具体的位置,将 $i(x, y, z)$ 投影到一维空间中,得到 $i(x_{(y,z)})$. S 的计算如式(1):

$$S = \sum_{i=1}^n \frac{(\deg^+ + \deg^-)}{2} \quad (1)$$

α_i 、 β_i 、 γ_i ($i=1, 2, 3$) 分别表示 M 、 I 和 S 在不同的 D_{DIK} 中所占的权重. $\Delta G_i(t, i, s)$ 是 TM 变化的差值, $\Delta F_i(t, i, s)$ 是 I 变化的差值, $\Delta H_s(t, i, s)$ 是 S 变化的差值. 式(2)分别计算综合已知的 M 、 I 和 S 值后得到的 U 、 R 、 C 的值:

$$\left. \begin{aligned} U &= e^{(\alpha_1 \Delta G_i(t, i, s) + \beta_1 \Delta F_i(t, i, s) + \gamma_1 \Delta H_s(t, i, s))} \\ R &= e^{(\alpha_2 \Delta G_i(t, i, s) + \beta_2 \Delta F_i(t, i, s) + \gamma_2 \Delta H_s(t, i, s))} \\ C &= e^{(\alpha_3 \Delta G_i(t, i, s) + \beta_3 \Delta F_i(t, i, s) + \gamma_3 \Delta H_s(t, i, s))} \end{aligned} \right\} \quad (2)$$

V 的计算如式(3)所示,其中 m 、 n 、 k 分别代表了 U 、 R 和 C 在 V 中所占的权重.

$$V(U, R, C) = e^{(mU + nR + kC)} \quad (3)$$

定义4 IG_{DIK}

$\text{IG}_{\text{DIK}}::=\text{Relative}_{\text{temporal|casual}} \{ D_{\text{DIK}} \}$

IG_{DIK} 记录资源之间的交互语义内容,以有向图的形式表示信息隐私资源之间的动态或因果关系(对承认和假定因果关系存在的情形).

定义5 KG_{DIK}

$\text{KG}_{\text{DIK}}::=\text{Assumption}_{\text{consistent}} \{ \text{Rule}_{\text{Probabilistic|Logical}} \}$

abstraction(Completeness)

KG_{DIK} 通过包含结点和结点之间关系的有向图来表达. KG_{DIK} 蕴含基于抽象得来的完整性假设或者基于概率统计的各种语义关系,能进行各种推理和概率计算.

2.3 体系化全类型化维度定义的资源

类型化数据分为静态类型化数据和动态类型化数据,一个具体事物(TH, Thing)由静态类型化数据和动态类型化数据组合后确定. 类型化数据: $\text{TH} = (T_A(T_{A1}(T_{A1A1}(\dots), T_{A1A2} \dots T_{A1An}), T_{A2} \dots T_{An}), T_B, T_C \dots T_N)$, T 代表一种类型,在 TH 的表达式中, T_A 子节点包括 $T_{A1}, T_{A2}, \dots, T_{An}$, T_{A1} 的子节点又有 $T_{A1A1} \dots T_{A1An}$, 每个维度都用一个类型表示. 基于体系化全类型化维度对隐私资源进行定义,例如,基于类型化数据定义数据隐私资源. 设定目标 D_{DIK} 隐私资源为操场上跑步的某个具体的人,通过此人移动设备所带的 GPS 获得其运动轨迹,静态的 D_{DIK} 包括 $T_{\text{occupation}}, T_{\text{sex}}$ 等,动态的 D_{DIK} 有 T_{movement} 等. $T_{\text{occupation}}$ 包括 $T_{\text{student}}, T_{\text{teacher}}, T_{\text{worker}}$. T_{sex} 包括 T_{male} 和 T_{female} . T_{student} 包括 $T_{\text{primary}}, T_{\text{senior}}, T_{\text{bachelor}}, T_{\text{master}}$ 和 T_{doctor} . 对于动态的 D_{DIK} 、 T_{movement} 包括 $T_{\text{walk}}, T_{\text{run}}$ 和 T_{swim} . 对于 T_{run} , 其 T_{speed} 是 6 km/min. 通过以上静态和动态的类型化数据组合,得知此人为 A : $A::=(T_{\text{occupation}}(T_{\text{student}}(T_{\text{maser}}), (T_{\text{sex}}(T_{\text{female}})), 6 = \text{INS}(T_{\text{speed}}))$.

2.4 资源转换机制

隐私保护方案的核心为转换机制,将目标隐私资源转换为其他类型化资源后,攻击者需要花费比破坏原隐私资源更多的代价来获取或攻击资源.

定义6 类型化资源转换(TRAN, Transformation) $\text{TRAN}::=\langle \text{TRAN}_{D-D}, \text{TRAN}_{D-I}, \text{TRAN}_{I-D}, \text{TRAN}_{I-I}, \text{TRAN}_{I-K}, \text{TRAN}_{K-I}, \text{TRAN}_{K-K} \rangle$.

这些转换分别对应通过概念映射和聚类对某种类型的资源进行处理,或者将其进行重组和分类等,重组后的资源集合对应不同的资源类型,由此得到不同的类型资源表达,并对应不同的资源存储量. 从而在处理前后面对不同的处理时空复杂度.

3 隐式隐私资源的保护

3.1 隐私保护

隐私分为广义隐私和狭义隐私,广义隐私是指不愿告诉他人的或不愿公开的个人或群体的事物、状态、活动或者可能被不被期望联系到的个人或群体存在的一切. 狭义隐私是指能够被关联到被保护目标的独具的存在的所有可能的资源. 在遍历所有类型化资源后,基于获得的完整资源分布求得资源对目标隐私的标识概率和程度. 资源的识别力计算公式为

$$D_p = \frac{N_{\text{indik}}}{N_{T_1}} \times \frac{N_{T_1}}{N_{T_2}} \times \cdots \times \frac{N_{T_1}}{N_{T_{i-1}}} \quad (4)$$

其中: N_{indik} 是遍历后获得的总的类型化资源数量, N_{T_1} 是符合第1个条件的类型化资源数量, N_{T_2} 是在 N_{T_1} 中符合第2个条件的类型化资源数量,直到获得符合最后一个条件的类型化资源数量 $N_{T_{i-1}}$. 隐私保护就是降低目标资源的识别力,或者增加确定和得到目标资源的计算时空代价.

3.2 显式和隐式隐私资源

定义7 显式和隐式类型化隐私资源

$\text{PR}_{\text{DIK}} ::= \langle \text{PR}_{\text{Type}}, \text{PR}_{\text{Scale}} \rangle$

$\text{PR}_{\text{Type}} ::= \{ \text{PD}_{\text{DIK}}, \text{PI}_{\text{DIK}}, \text{PK}_{\text{DIK}} \}$, 类型化隐私资源 PR_{DIK} 包括数据隐私资源 PD_{DIK} , 信息隐私资源 PI_{DIK} , 知识隐私资源 PK_{DIK} . 每一种类型化隐私资源都有对应的资源规模 PR_{Scale} . 在 PR_{DIK} 的定义基础上,进一步将目标 PD_{DIK} 、 PI_{DIK} 和 PK_{DIK} 按照其在搜索空间中的类型存在形式分类为显式和隐式的情形. 显式和隐式隐私资源定义如表1所示.

表1 显式和隐式类型化隐私资源定义

类型	D_{DIK}	I_{DIK}	K_{DIK}
显式	$\text{PD}_{\text{DIK}}^{\text{EX}} = \{ dx_n \}$	$\text{PI}_{\text{DIK}}^{\text{EX}} = \{ ix_n \}$	$\text{PK}_{\text{DIK}}^{\text{EX}} = \{ kx_n \}$
隐式	$\text{PD}_{\text{DIK}}^{\text{IM}} = \{ dx_n \}$	$\text{PI}_{\text{DIK}}^{\text{IM}} = \{ ix_n \}$	$\text{PK}_{\text{DIK}}^{\text{IM}} = \{ kx_n \}$

显式和隐式类型化隐私资源总共包括6种,即显式数据隐私资源 $\text{PD}_{\text{DIK}}^{\text{EX}}$, 隐式数据隐私资源 $\text{PD}_{\text{DIK}}^{\text{IM}}$, 显式信息隐私资源 $\text{PI}_{\text{DIK}}^{\text{EX}}$, 隐式信息隐私资源 $\text{PI}_{\text{DIK}}^{\text{IM}}$, 显式知识隐私资源 $\text{PK}_{\text{DIK}}^{\text{EX}}$ 和隐式知识隐私资源 $\text{PK}_{\text{DIK}}^{\text{IM}}$.

3.3 交互代价驱动的转换

交互代价驱动的安全保护方法(C_{ICP})包含5个算法: $C_{\text{ICP}} = (\text{INF}(), \text{FIND}(), \text{COUNT}_{\text{Tran}}(), \text{COUNT}_{\text{Com}}(), \text{OP}())$,在确定隐私保护框架中投资

者的期望代价 C_p 和攻击者的期望代价 C_A 后,用优化函数 $\text{OP}()$ 选出最小化投资者投入同时能最大化投资者保护效果的转换方式,即 $\text{OP}(C_A, C_p) = \text{Maximum}(C_A/C_p)$:

1) $\text{INF}(\text{PR}_{\text{Type}}) \rightarrow M[\text{INF}_{\text{PR1}}, \text{INF}_{\text{PR2}} \cdots \text{INF}_{\text{PRn}}]$: 影响力计算函数 $\text{INF}()$,在输入不同类型的 PR_{Type} 后,计算出每个节点的影响力大小,并将影响力计算结果 INF_{PRn} 按从大到小的顺序存入数组 M .

2) $\text{FIND}(M) \rightarrow \text{COLLECTION}\{\text{PR}_{\text{DIK}}'\}$: 寻找路径函数 $\text{FIND}()$ 在通过 $\text{INF}()$ 得到数组 M 后,依次寻找 M 中的各节点转换为其他隐私资源 PR_{DIK}' 的转换路径,将该节点的所有转换路径保存,得到 $\text{COLLECTION}\{\text{PR}_{\text{DIK}}'\}$. 例如 D_{DIK} 存在于 DG_{DIK} 上,同时,通过 IG_{DIK} 上的 I_{DIK} 和 KG_{DIK} 上的 K_{DIK} 也能得到 D_{DIK} .

3) $\text{COUNT}_{\text{Tran}}(M, \text{COLLECTION}\{\text{PR}_{\text{DIK}}'\}) \rightarrow C_{\text{Tran}}$: 转换代价计算函数 $\text{COUNT}_{\text{Tran}}()$ 根据 $\text{INF}()$ 得到的数组 M 和 $\text{FIND}()$ 函数得到的 $\text{COLLECTION}\{\text{PR}_{\text{DIK}}'\}$,对 PR_{DIK} 的转换代价 C_{Tran} 进行计算.

4) $\text{COUNT}_{\text{Com}}(M) \rightarrow C_{\text{Com}}$: 保护代价计算函数 $\text{COUNT}_{\text{Com}}()$ 由破坏结点的代价和搜索代价组成.

5) $\text{OP}(C_A, C_{\text{Tran}}, C_{\text{Com}}, C_p) \rightarrow P_i$: 最优转换方式选择函数 $\text{OP}()$ 在输入 C_{Tran} 和 C_{Com} 后,计算出目标隐私资源转换所需的总的代价 C_{Tot} , $C_{\text{Tot}} = C_{\text{Tran}} + C_{\text{Com}}$. 此后比较 C_{Tot} 与 C_A ,用最小的代价实现投资者隐私保护最大化.

4 保护案例示意

模拟了一个基于校园监控系统展示保护情形. 假设用户的目标 PD_{DIK} 为身份,通过用户自身携带移动设备获取用户 GPS 信息,如图1所示,目标 PD_{DIK} 无法在 DG_{DIK} 上被直接遍历得到,即目标 PD_{DIK} 是 $\text{PD}_{\text{DIK}}^{\text{IM}}$. {学校南门}, {学生食堂} 和 {图书馆} 被分类为 DG_{DIK} 上的 PD_{DIK} , PD_{DIK} 交互形成的移动轨迹构成了动态的 $\text{PI}_{\text{DIK1}} = \{ \text{学校南门到学生食堂到图书馆} \}$ 和 $\text{PI}_{\text{DIK2}} = \{ \text{用户刷了校园卡坐校车} \}$,再结合 KG_{DIK} 上的 $\text{K}_{\text{DIK1}} = \{ \text{刷校园卡的是学校学生或者员工} \}$ 以及 $\text{K}_{\text{DIK2}} = \{ \text{学生在学生食堂就餐} \}$,知识推理分析得到目标 $\text{PD}_{\text{DIK}}^{\text{IM}}$ 是学生. 保护目标隐式数据隐私资源 $\text{PD}_{\text{DIK}}^{\text{IM}}$ 时,根据 $\text{FIND}()$ 找到两条转换路径,即通过 $\text{TRAN}_{\text{K-D}}$ 转换的路径和通过 $\text{TRAN}_{\text{I-D}}$ 转换的路径,转换后的2条路径皆可定位到 DG_{DIK} 中推出目标 $\text{PD}_{\text{DIK}}^{\text{IM}}$. 据 $\text{OP}()$ 选出两条转换路径中 C_{tot} 最小

的方案进行目标 PD_{DIK}^{IM} 的转换, 并将转换的 PR_{DIK} 存入安全空间。

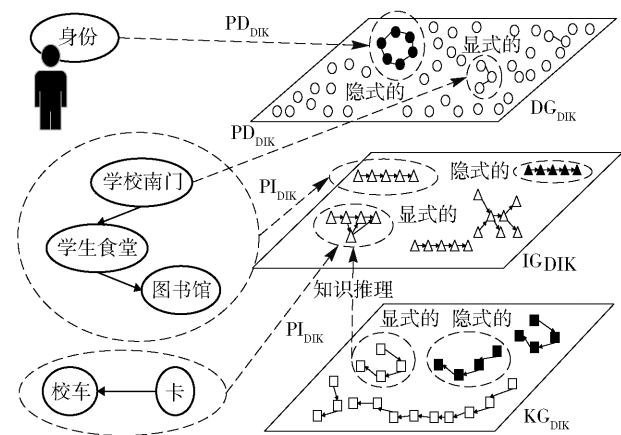


图1 目标隐式数据隐私资源 (PI_{DIK}^{EX})

5 结束语

基于关系定义一切语义的语义表述建模模型和存在计算层面的语义基础推理机制, 给出了类型化 DIKW 相关概念的语义概念表达元模型。将目标隐私资源对应分类为 DIKW 架构中的数据、信息和知识等类型化资源。其中类型化数据资源由多维度的频度综合标定。分别将类型化隐私资源根据在隐式与显式的场景中的存在形式分为隐式隐私资源和显式隐私资源。提出价值导向的保护解决方案, 采用交互代价驱动的保护方法选择最优的类型转换方案和计算并确定转换程度。

参考文献:

- [1] Chattopadhyay E, Li X. Explicit non-malleable extractors, multi-source extractors, and almost optimal privacy amplification protocols[C] // FOCS'16. New Brunswick: IEEE, 2016: 158-167.
- [2] Rahmati A, Fernandes E, Eykholt K, et al. Heimdall: A Privacy-Respecting implicit preference collection framework [C] // MobiSys'17. New York: ACM, 2017: 453-463.
- [3] Duan Y, Shao L, Hu G, et al. Specifying architecture of knowledge graph with data graph, information graph, knowledge graph and wisdom graph [C] // SERA'17. London: IEEE, 2017: 327-332.
- [4] Hundepool A, Domingo-Ferrer J, Franconi L, et al. De Wolf[M]. John Wiley & Sons: [s. n.], 2012.
- [5] Pearson S, Charlesworth A. Accountability as a way forward for privacy protection in the cloud [C] // IEEE CLOUD'09. Berlin: Springer, 2009: 131-144.
- [6] Mcsherry F D. Privacy integrated queries: an extensible platform for privacy-preserving data analysis [J]. Commun ACM, 2010, 53(9): 89-97.
- [7] 刘峤, 李杨, 段宏, 等. 知识图谱构建技术综述[J]. 计算机研究与发展, 2016, 53(3): 582-600.
- [8] Liu Qiao, Li Yang, Duan Hong, et al. Knowledge graph construction techniques [J]. Journal of Computer Research & Development, 2016, 53(3): 582-600.
- [9] Zins C. Conceptual approaches for defining data, information, and knowledge[J]. JSIST, 2010, 58(4): 479-493.
- [10] Rowley J. The wisdom hierarchy: representations of the DIKW hierarchy[J]. J Inf Sci, 2010, 33(2): 163-180.
- [11] Duan Y, Sun X, Che H, et al. Modeling data, information and knowledge for security protection of hybrid IoT and edge resources[J]. IEEE Access, 2019(7): 99161-99176.
- [12] Sowa J F. Knowledge representation: logical, philosophical and computational foundations [M]. [S. l.]: Brooks/Cole Publishing Co., 1999.
- [13] Samani A, Ghenniwa H H, Wahaishi A. Privacy in internet of things: a model and protection framework [J]. Procedia Computer Science, 2015(52): 606-613.
- [14] Kant I. Critique of pure reason [J]. JHP, 1998, 2(656): 1.
- [15] Duan Y. Towards a periodic table of conceptualization and formalization on state, style, structure, pattern, framework, architecture, service and so on [C] // IEEE SNPD'19. Toyama: IEEE, 2019: 133-138.
- [16] Duan Y. Existence computation: revelation on entity vs. relationship for relationship defined everything of semantics [C] // IEEE SNPD'19. Toyama: IEEE, 2019: 139-144.
- [17] Schopenhauer A. The world as will and presentation: volume I [M]. [S. l.]: Dover Publications, 2016.