

带权重谓词的可选事务逻辑及其访问控制应用

马莉¹ 霍颖瑜¹ 钟勇¹ 秦小麟²

(佛山科学技术学院电子与信息工程学院 佛山 528000)¹

(南京航空航天大学信息安全研究所 南京 210016)²

摘要 逻辑语言由于其表达力和灵活性,是访问控制中授权语言的基础之一。针对 Datalog 语言缺乏表达事务和多方决策模型的能力,对 Datalog 进行了扩展,提出了一种带权重谓词的可选事务逻辑 WT-Logic。首先对 WT-Logic 的语法、语义进行了说明;然后解释了其评价方法;最后对 WT-Logic 语言在工作流授权和多方投票机制中的应用进行了描述和示例,说明了 WT-Logic 的表达力和可应用性。

关键词 可选事务逻辑,权重谓词,WT-Logic,Datalog,授权语言

中图分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.10.033

Optional Transaction Logic with Weighted Predicates and its Application in Access Control

MA Li¹ HUO Ying-yu¹ ZHONG Yong¹ QIN Xiao-lin²

(School of Electronic and Information Engineering, Foshan University, Foshan 528000, China)¹

(Institute of Information Security, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)²

Abstract Due to the expressiveness and flexibility, logic languages have become one of the bases of authorization language in access control. Concerned on the ability to express transaction and multi-party decision model, this paper extended Datalog language to WT-Logic, which is a kind of optional transaction logic with weighted predicates. Firstly, the syntax and semantics of the logic are discussed. Secondly, the evaluation method of the logic is explained. Lastly, the application of WT-logic in workflow authorization and multi-party voting mechanism is described and exemplified, which shows the expressiveness and application of the logic.

Keywords Optional transaction logic, Weighted predicates, WT-Logic, Datalog, Authorization language

1 引言

在访问控制和信息安全研究领域,逻辑语言由于其表达力和灵活性,往往作为授权语言的基础。如 Vera 等^[1]提出的基于 Datalog 的分布式数据管理框架,几乎具有一阶逻辑表达力的授权语言;Liu 等^[2]将负 Datalog 应用于基于角色的访问控制模型;Galland 等^[3]将 Datalog 语言应用于社交网络访问控制;我们在前期研究中提出的 LucScript 权利描述语言等模型^[4,5]均采用逻辑语言作为授权语言的基础。逻辑语言作为授权语言的基础需要解决推理的确定性和表达力之间的矛盾以及推理的复杂度也即实现的可行性问题,如 Prolog 语言虽然具有一阶谓词逻辑的表达力,但因为不具有推理的确定性而难以应用于授权语言中。

Datalog 逻辑语言由于在表达力、灵活性和语义完整性以及确定性上的优势使其成为授权语言中广泛应用的逻辑语言。但 Datalog 语言由于其表达力的限制因而在一些领域的

应用受到限制,如 Datalog 语言由 Horn 子句构成,不具有事务概念,难以表达工作流授权中的事务和执行顺序语义。我们在研究社交网络多方访问控制^[6,7]问题中也发现,现有的 Datalog 语言难以建立多方决策模型,如无法表达授权权重、无法实现多方投票、主体可选等概念。

在现有的相关逻辑中,事务逻辑(Transaction Logic)^[8,9]具有表达事务和执行顺序的能力,但事务逻辑中没有可选谓词的概念,也不能表达授权权重,无法表达多方投票的概念。本质上,Datalog 语言是一阶谓词逻辑中子句逻辑的子集,是 Horn 子句逻辑的受限形式,是 Prolog 语言的子集,Prolog 语言虽然具有一阶谓词逻辑的表达力,但仍不具有表达事务和多方授权能力。Active-U-Datalog^[10,11]是结合主动规则具有可更新能力的扩展 Datalog 程序,是目前最具表达力的扩展 Datalog 语言,但其表达力仍未超出 Prolog 语言范畴。因而,本文提出一种能表达事务概念、具有谓词权重的扩展 Datalog 语言 WT-Logic,该语言的主要优势在于:

到稿日期:2015-09-18 返修日期:2016-01-31 本文受国家自然科学基金(61373015,11326123),国家星火计划(2014GA780031),广东省自然科学基金项目(2015A030313638),佛山市科技发展专项资金项目(2012AA100251)资助。

马莉(1977—),女,硕士,副教授,主要研究方向为形式化方法、信息安全、访问控制等;霍颖瑜(1979—),女,硕士,讲师,主要研究方向为社交网络访问控制、信息安全,E-mail: foshuhy@163.com;钟勇(1970—),男,博士,教授,主要研究方向为信息安全、访问控制、数字版权保护技术等;秦小麟(1953—),男,教授,博士生导师,主要研究方向为安全数据库、空间数据库、时空数据库、信息安全等。

(1)将权重谓词和可选谓词原子引入 Datalog 规则,使 Datalog 规则具有建立多方决策模型的能力;

(2)将事务概念引入 Datalog 语言,通过复合事务实现了 Datalog 语言表达执行顺序的能力。

本文对 WT-Logic 的语法、语义进行了说明,解释了其评价方法,并对其在工作流访问控制和多方投票规则中的应用进行了说明和示例。

2 WT-Logic 的语法

2.1 原子公式和原子类型

(1)定义单个常量是项

(2)定义单个变量是项

使 $p(x_1, \dots, x_n)$ 中的 p 为任意谓词符号, $x_1, \dots, x_n$ 是相应取值域上的项,称 $p(x_1, \dots, x_n)$ 或 $\pm p(x_1, \dots, x_n)$ 是一个原子公式 P (简称原子),其包括两类原子: 1) 查询原子,称 $p(x_1, \dots, x_n)$ 为查询原子; 2) 更新原子, $\pm p(x_1, \dots, x_n)$ 分别表示相应外延谓词的插入和删除,称为更新原子。

2.2 事务和程序

定义 1(程序) 程序 $PR = IDB \cup EDB$, 其中外延数据库 EDB 由代表数据库状态的外延基原子 (ground atom) 集组成, 内涵数据库 IDB 是由下列形式规则组成的集合:

$$w_0: P_0 \leftarrow w_1: P_1, \dots, w_k: P_k, [w_{k+1}: P_{k+1}], \dots, [w_n: P_n], \\ u_1, \dots, u_m \quad (1)$$

其中, $w_i (0 \leq i \leq n)$ 是非负实数, 称为权重, $P_i (0 \leq i \leq n)$ 是查询原子, 称中括号 $[]$ 内的谓词原子为可选查询原子, $U_i (1 \leq i \leq m)$ 是更新原子。

$w_i (0 \leq i \leq n)$ 缺省表示权重为 0 的状态, 因而传统的 Datalog 规则是 WT-Logic 规则的特例。

定义 2(原子事务) 原子事务 T 是不含规则头的具有如下形式的规则:

$$w_1: P_1, \dots, w_k: P_k, [w_{k+1}: P_{k+1}], \dots, [w_n: P_n], U_1, \dots, U_m \quad (2)$$

其中, $w_i (1 \leq i \leq n)$ 是非负实数, 称为权重, $P_i (1 \leq i \leq n+m)$ 是谓词原子, 称中括号 $[]$ 内的谓词原子为可选谓词原子。

定义 3(查询事务) 查询事务 Q 是不含规则头的具有如下形式的规则:

$$w_0: (w_1: P_1, \dots, w_k: P_k, [w_{k+1}: P_{k+1}], \dots, [w_n: P_n], U_1, \dots, U_m) \quad (3)$$

其中, $w_i (0 \leq i \leq n)$ 是非负实数, 称为权重, $P_i (1 \leq i \leq n)$ 是谓词原子, 称中括号 $[]$ 内的谓词原子为可选谓词原子。本文使用 $-w_0: (w_1: P_1, \dots, w_k: P_k, [w_{k+1}: P_{k+1}], \dots, [w_n: P_n], U_1, \dots, U_m)$ 表示查询事务, 简称查询。如果 w_0 等于零, 则查询事务等同于原子事务。

定义 4(复合事务) 复合事务 CT 是具有如下形式的规则:

$$w_1: t_1 \otimes w_2: t_2 \dots \otimes w_n: t_n \quad (4)$$

其中, $w_i (0 \leq i \leq n)$ 是大于或等于零的实数, 称为权重, $t_i (1 \leq i \leq n)$ 是原子事务。图 1 分别是原子事务、查询事务和复合事务示例:

原子事务 T :

$$(reviewer(R, 1), 1; accept(R, P))$$

查询事务 QT :

$$1; (reviewer(R, 1), 1; accept(R, P))$$

复合事务 CT :

$$1; (reviewer(R, 1), 1; accept(R, P)) \quad 10; (reviewer(R, 2), \\ [N; score(R, P, N)], score(R, P, N), N2) \quad 8; (reviewer(R, 3), \\ [N; score(R, P, N)], score(R, P, N), N3)$$

图 1 事务示例

在复合事务中, 如果 $w_i (0 \leq i \leq n)$ 等于零, 可以将 $w_i: t_i$ 视为原子事务, 省略 w_i , 对于只具有单点谓词的原子事务, 也可以省略事务的外括号, 如式(5)、式(6)的复合事务指的是同一事务:

$$(reviewer(R, 1), 1; accept(R, P)) \otimes 10; pass(P, 2) \otimes 8; \\ (N; score(R, P, N)) \quad (5)$$

$$0; (reviewer(R, 1), 1; accept(R, P)) \otimes 0; (10; pass(P, 2)) \otimes 8; \\ (N; score(R, P, N)) \quad (6)$$

3 WT-Logic 的语义

定义扩展的 Herbrand 基 β^+ 包含如下形式的文字: $P \leftarrow \tilde{u}$, 其中 P 是查询原子 ($IDB \cup EDB$), $\tilde{u}$ 是更新原子的合取式^[10]。

通过定义自底向上的算子 T 说明 WT-Logic 的语义。简单起见, 不考虑规则体中包括负文字的情况, 负文字的处理可以采取分层(stratified)^[12, 13]等传统方法处理。

定义 5(更新相容性) 设 $PR = EDB \cup IDB$ 是 WT-Logic 程序, 更新集 $\tilde{u} = \{u_1, u_2, \dots, u_n\}$, 称更新集 $\tilde{u}$ 与外延数据库 EDB 具有更新相容性, 当且仅当下列条件满足:

(1) $\forall \delta p(\tilde{t}) \in \tilde{u} \Rightarrow \exists \gamma p(\tilde{t}) \in \tilde{u} \wedge \delta \neq \gamma$, 其中 $\delta, \gamma \in \{+, -\}$ 。

(2) $\forall +p(\tilde{t}) \in \tilde{u} \Rightarrow p(\tilde{t}) \notin EDB$ 。

(3) $\forall -p(\tilde{t}) \in \tilde{u} \Rightarrow p(\tilde{t}) \in EDB$ 。

更新集 $\tilde{u}$ 与外延数据库 EDB 具有更新相容性, 表示为 $EDB|_c \tilde{u}$, 为方便起见, 有时也表示为 $PR|_c \tilde{u}$ 。

定义 6(直接操作算子) 设 PR 是 WT-Logic 程序, I 是一个解释(interpretation), 则定义 T 算子 ($2^{\beta^+} \rightarrow 2^{\beta^+}$) 如下:

$$T(I) = \{P \leftarrow \tilde{u}' \mid \exists \text{ 重命名规则}$$

$$w_0: P_0(\tilde{t}) \leftarrow w_1: P_1(\tilde{X}_1), \dots, w_k: P_k(\tilde{X}_k), [w_{k+1}: P_{k+1}(\tilde{X}_{k+1}), \dots, [w_n: P_n(\tilde{X}_n)], \tilde{u} \in PR$$

$$w\tilde{u} = \sum_{i=1}^k w_i \mid (\forall i=1, \dots, k, \exists \theta (P_i(\tilde{X}_i) \leftarrow \tilde{u}_i) \in I)$$

$$w\tilde{u} = \sum w_i, \tilde{u}_i = \bigwedge_j \tilde{u}_j \mid \forall P(\tilde{Y}) \leftarrow \tilde{u}_j \in I \wedge \exists i \in \{k+1, \dots, n\}, \exists \theta \theta P(\tilde{Y}) = P_i(\tilde{X}_i))$$

$$w\tilde{u} + w\tilde{u} \geq w_0$$

且在不共享变量的情况下有 $p(\tilde{X}) = \theta p(\tilde{t})$

$$\tilde{u}' = (\bigwedge_i \tilde{u}_i \wedge \tilde{u}) \theta$$

$$PR|_c \tilde{u}'$$

}

(7)

直接算子 $T(I)$ 说明规则的成立要求任意规则体中的查询文字 $P_i(\tilde{Y}_i) \leftarrow \tilde{u}_i (1 \leq i \leq k)$, 如果经变量通代 (θ) 后即 $\theta P_i(\tilde{Y}_i)$ 属于解释 I , 那么累加该文字的权重 w_i 到 w_t 中。对解释 I 中的任何文字 $\forall P(\tilde{Y})$ 经变量通代 (θ) 后能够等于规则中的任意可选查询原子 $P_i(\tilde{X}_i) (k+1 \leq i \leq n)$, 则累积该文字的权重 w_i 到 w_u 中, 最终需要 $w_t + w_u$ 大于或等于 w_0 。

可选查询原子在解释中的成立不是必须的, 但是是可以累积的, 如对解释 $I = \{p(a), q(b), r(a), r(b)\}$, 对如下的 WT-Logic 规则:

$$3: q(x) \leftarrow 1: p(x), [1: r(y)] \quad (8)$$

x 绑定后有如下规则:

$$3: q(a) \leftarrow 1: p(a), [1: r(y)] \quad (9)$$

解释 I 中 $r(a)$ 和 $r(b)$ 让可选文字成立两次, 有 $w=3$, 规则成立, 因而 $T(I) = \{p(a), q(a), q(b), r(a), r(b)\}$ 。

定理 1 (固定点存在定理) 设 PR 是 WT-Logic 程序, T 是直接操作算子, 直接操作算子 T 存在固定点, 即固定点 $Fix(PR) = T_{PR} \uparrow \omega$ 。

文献[10]说明了在 U-Datalog 中以及在 CLP(Constraint Logic Programming) 程序中该定理的正确性。假定 $T_p(I)$ 是 U-Datalog 中的直接操作算子, 在 U-Datalog 中有:

$$I_1 \subseteq I_2 \Rightarrow T_p(I_1) \subseteq T_p(I_2) \quad (10)$$

$T_1(I)$ 是在 $T_p(I)$ 的基础上增加了对权重的限制条件, 用函数 $F(T_p(I))$ 表示该限制条件, 只需要证明:

$$I_1 \subseteq I_2 \Rightarrow F(T_p(I_1)) \subseteq F(T_p(I_2)) \quad (11)$$

对任意事实 $P(\tilde{t}) \leftarrow \tilde{u} \in F(T_p(I_1))$, 假定该事实由规则 $w: P(\tilde{t}) \leftarrow w_1: P_1(\tilde{X}_1), \dots, w_k: P_k(\tilde{X}_k), [w_{k+1}: P_{k+1}(\tilde{X}_{k+1})], \dots, [w_n: P_n(\tilde{X}_n)]$ 推出, 那么对任意 $P_i(\tilde{X}_i), \theta(P_i(\tilde{X}_i) \leftarrow \tilde{u}_i) \in I_1 \Rightarrow \theta(P_i(\tilde{X}_i) \leftarrow \tilde{u}_i) \in I_2$, 这是由于 $I_1 \subseteq I_2$, 在 I_2 中 w 的值只会不小于 I_1 中 w 的值, 也即 $w_{i_2} \geq w_{i_1}$, 因而 $P(\tilde{t}) \leftarrow \tilde{u} \in F(T_p(I_2))$, 即下列规则成立:

$$P(\tilde{t}) \in F(T_p(I_1)) \Rightarrow P(\tilde{t}) \in F(T_p(I_2)) \quad (12)$$

由规则(12)可推出 $F(T_p(I_1)) \subseteq F(T_p(I_2))$, 规则(11)得证, 也即定理 1 得证。

例 1 设有 WT-Logic 程序如图 2 所示, 使用直接操作算子得到的结果:

1. $T_0(PR) = \{q(b), t(a), r(a), r(b)\}$
2. $T_1(PR) = \{p(b)\} \cup T_0(PR)$
3. $T_2(PR) = \{h(b) \leftarrow +t(b)\} \cup T_1(PR)$
4. $T_3(PR) = \{s(a) \leftarrow -t(a)\} \cup T_2(PR)$
5. $T_4(PR) = T_3(PR) = Fix(PR)$

按照定理 1: $Fix(PR) = T_3(PR)$ 。

```
q(b); t(a), r(a), r(b); //EDB
3: p(x) ← 1: q(x), [1: r(y)]
0: h(X) ← +t(X), 0: p(X);
2: s(X) ← 1: t(X), [1: r(X)], -t(a); //IDB
```

图 2 WT-Logic 程序示例

4 评价方法

定义 7^[11] (绑定算子 $b_{|T}$ 和替换算子 $eqn(\theta)$) 给定绑定集 b 和事务 T , 定义绑定算子 $b_{|T}$:

$$b_{|T} = \{(X=t) \in b \mid X \text{ 在 } T \text{ 中出现}\} \quad (13)$$

给定替换 $\theta = \{V_1 \leftarrow t_1, \dots, V_n \leftarrow t_n\}$, 定义替换算子 $eqn(\theta)$:

$$eqn(\theta) = \{V_1 = t_1, \dots, V_n = t_n\} \quad (14)$$

定义 8 (原子事务的更新集) 给定 WT-Datalog 程序 PR 及其固定点 $Fix(PR)$ 、原子事务 $T = ?-(w_1: P_1, \dots, w_k: P_k, [w_{k+1}: P_{k+1}], \dots, [w_n: P_n], \tilde{u}_0)$, 定义在固定点 $Fix(PR)$ 语义下 T 在 PR 中的更新集 $Set_{-u}^{\wedge}(T, PR)$:

$$Set_{-u}^{\wedge}(T, PR) = \{\tilde{u} \mid A_i \leftarrow \tilde{u}_i \in Fix(PR), 1 \leq i \leq n$$

$$\theta = mgu((P_1, \dots, P_n), (A_1, \dots, A_n))$$

$$\tilde{u} = (\tilde{u}_0, \tilde{u}_1, \dots, \tilde{u}_n) \theta\} \quad (15)$$

定义 9 (原子事务的可成立性和事务成立权重) 给定 WT-Datalog 程序 $PR = EDB \cup IDB$ 、原子事务 $T = ?-(w_1: P_1, \dots, w_k: P_k, [w_{k+1}: P_{k+1}], \dots, [w_n: P_n], \tilde{u}_0)$, 定义事务的可成立性:

(1) 如 $\forall P_i (1 \leq i \leq k) \Rightarrow P_i \in Fix(PR)$, 则称事务 T 对程序 PR 是查询可成立的, 表示为 $PR \models_q T$;

(2) 如 $PR \models_q T \wedge PR \models_c Set_{-u}^{\wedge}(T, PR)$, 则称原子事务 T 对程序 PR 是可成立的, 表示为 $PR \models T$ 。

定义 10 (事务成立权重) 给定 WT-Datalog 程序 PR 及其固定点 $Fix(PR)$ 、事务 $T = w_0: (w_1: P_1(\tilde{X}_1), \dots, w_k: P_k(\tilde{X}_k), [w_{k+1}: P_{k+1}(\tilde{X}_{k+1})], \dots, [w_n: P_n(\tilde{X}_n)], \tilde{u}_0)$, 如果 $PR \models T$, 则定义在固定点 $Fix(PR)$ 语义下 T 在 PR 中的事务成立权重 $W(PR, T)$:

$$W(PR, T) = \{wt + wu \mid \exists \text{ 替换 } \theta$$

$$wt = \sum_{i=1}^k w_i \mid (\forall i = 1, \dots, k, \exists \theta(P_i(\tilde{X}_i) \leftarrow \tilde{u}_i) \in Fix(PR))$$

$$wu = \sum w_i, \tilde{u}_i = \bigwedge_j \tilde{u}_j \mid \forall P(\tilde{Y}) \leftarrow \tilde{u}_j \in Fix(PR) \wedge \exists i \in \{k+1, \dots, n\}, \exists \theta \theta P(\tilde{Y}) = P_i(\tilde{X}_i)\}$$

(16)

定义 11 (查询事务的可成立性) 给定 WT-Datalog 程序 $PR = EDB \cup IDB$ 、原子事务 $T = w_0: (w_1: P_1, \dots, w_k: P_k, [w_{k+1}: P_{k+1}], \dots, [w_n: P_n], \tilde{u}_0)$, 定义查询事务的可成立性: $PR \models T \wedge W(PR, T) \geq w_0$, 则称查询事务 T 对程序 PR 是事务可成立的, 表示为 $PR \models T$ 。

定义 12 (事务执行蕴含) 给定 WT-Datalog 程序 $PR = EDB \cup IDB$ 、事务 T 是 PR 的可成立性事务, 定义事务 T 在程序 PR 中的执行蕴含: $IDB, B, B' \mid = T$, 其中 $B = EDB, B'$ 是事务 T 执行后的外延数据库, 显然, 对更新原子 $p(\tilde{t})$ 有:

$$IDB, EDB, EDB \cup \{p(\tilde{t})\} \mid = \{+p(\tilde{t})\} \quad (17)$$

$$IDB, EDB, EDB \setminus \{p(\tilde{t})\} \mid = \{-p(\tilde{t})\} \quad (18)$$

定义 13 (复合事务的可成立性) 给定 WT-Datalog 程序 $PR = EDB \cup IDB$ 、复合事务 $T = w_1: t_1 \otimes w_2: t_2 \otimes \dots \otimes w_n: t_n$, 定义复合事务 T 的可成立性:

$$(1) EDB \cup IDB \mid = w_1: t_1 \wedge IDB, EDB, B_1 \mid = t_1;$$

$$(2) EDB \cup B_1 \mid = w_2: t_2 \wedge IDB, B_1, B_2 \mid = t_2;$$

$$(3) \forall 2 \leq i \leq n-1, EDB \cup B_i \mid = w_{i+1}: t_{i+1} \wedge IDB, B_i, B_{i+1} \mid = t_{i+1};$$

则称原子事务 T 对程序 PR 是可成立的, 表示为 $PR \models T$, 复合事务的可成立性表示为 $IDB, EDB, B_n \mid = T$ 。

5 应用示例

5.1 工作流授权

某期刊论文采取三审制,初审对稿件格式进行审查,二审由 3 位专家进行评分,终审由 2 位终审专家打分确定最终结果。评分标准采取五分制,二审通过须得分 10 以上,但不能有一个专家给予 2 分以下;终审二位专家的评分均须超过 3 分且总分不少于 8 分;通过三审的稿件,总分超过 23 分以上的是优,20 分以上的是良,其余的是接受。

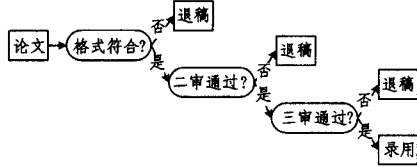


图 3 审稿流程

外延数据库 EDB

reviewer(john, 1), reviewer(mary, 2), reviewer(bob, 2), reviewer(mike, 2), reviewer(nick, 3), reviewer(jerry, 3) (1)

内涵数据库 IDB:

1:pass(P,1)←reviewer(R,1),1:format(R,P,TRUE) (2)

10:pass(P,2)←reviewer(R,2),[N:score(R,P,N)],score(R,P,N),N2 (3)

8:pass(P,3)←reviewer(R,3),[N:score(R,P,N)],score(R,P,N),N3 (4)

pass(P)←pass(P,1),pass(P,2),pass(P,2) (5)

23:label(P,“excellent”)←[N:score(R,P,N)],pass(P) (6)

20:label(P,“good”)←[N:score(R,P,N)],pass(P) (7)

conclusion(P,“deny”)←pass(P) (8)

conclusion(P,“excellent”)←label(P,“excellent”) (9)

conclusion(P,“good”)←label(P,“good”),label(P,“excellent”) (10)

conclusion(P,“accept”)←pass(P),label(P,“good”),label(P,“excellent”) (11)

review(P,1)←reviewer(R,1),INPUT(R,P,result),+format(R,P,result) (12)

review(P,2)←reviewer(R,2),INPUTScore(R,P,sc),+score(R,P,sc) (13)

review(P,3)←reviewer(R,3),INPUTScore(R,P,sc),+score(R,P,sc) (14)

复合事务 CT:

1:pass(P,1)10:pass(P,2)8:pass(P,3)conclusion(P,R) (15)

图 4 工作流授权程序示例

图 4 中外延数据库 EDB 语句(1)说明 6 位审稿专家各自负责的评审阶段。内涵数据库 IDB 规则(2)说明一位一审专家进行格式审查后同意则论文通过了一审;规则(3)说明二审专家打分累积 10 以上,且不存在不高于 2 分的得分则论文通过了二审;规则(4)说明三审专家打分累积 8 以上,且不存在不高于 3 分的得分则论文通过了三审;规则(5)说明三审都通过了,则论文通过评审;规则(6)说明如果通过评审且总分超过 23 分则将论文标记为“excellent”;规则(7)说明如果通过评审且总分超过 20 分则将论文标记为“good”;规则(8)说明如果论文未通过评审,则审稿结论为“deny”;规则(9)说明如果论文已被标记为“excellent”,则审稿结论为“excellent”;规则(10)说明如果论文已被标记为“good”且未标记为“excel-

lent”,则审稿结论为“good”;规则(11)说明如果论文通过但未被标记为“good”和“excellent”,则审稿结论为“accept”;规则(12)~规则(14)说明了审稿专家的审稿过程,通过更新原子将审稿结论插入 EDB 中;复合事务 CT 语句(15)是审稿过程,通过审稿过程后的最终结论存放在 conclusion(P,R)中。

图 4 中的负文字可按表 1 分层,因而也是可评价的。

表 1 审稿系统谓词分层

层	谓词	规则体包含谓词
1	外延谓词 P _{ext}	外延谓词 P _{ext} 包括 reviewer, score, format 等谓词
2	review 规则	外延谓词 P _{ext}
3	pass 规则	外延谓词 P _{ext}
4	label 规则	外延谓词 P _{ext} , pass 文字
5	conclusion 规则	外延谓词 P _{ext} , pass 和 label 文字

图 4 的程序说明了 WT-Logic 能表示传统逻辑语言无法表达的复杂工作流程授权。

5.2 多方投票机制应用示例

WT-Logic 逻辑能表达复杂的投票机制,如某董事会具有下列议事规则:

(1)公司重大事务。必须所有董事都同意。

(2)公司重要事务。必须由 2/3 的董事通过且董事长未否决才能通过。

(3)公司一般事务。必须多数董事同意。

(4)公司部门事务。不同职位的董事具有不同的投票权重,累积权重超过事务预先确定的权重如 W 则通过。

分别用 T_{重大}、T_{重要}、T_{一般}和 T_{部门}表示事务集,BOARD 表示董事会成员集,主要程序如图 5 所示。

N:Pass(t)←t∈T_{重大},s∈BOARD,[1:Vote(s,t,true)],Sumof(BOARD,N) (1)

2/3 * N:Pass(t)←t∈T_{重要},s∈BOARD,[1:Vote(s,t,true)],Sumof(BOARD,N),vote(CHAIR,t,true) (2)

1/2 * N:Pass(t)←t∈T_{一般},s∈BOARD,[1:Vote(s,t,true)],Sumof(BOARD,N),vote(CHAIR,t,true) (3)

W: Pass(t)←t∈T_{部门},s∈BOARD,[w:Vote(s,t,true)],position(s,w) (4)

图 5 多方投票决策程序示例

图 5 中规则(1)说明所有投票者必须都同意,其中谓词 Sumof 计算董事会人数;规则(2)说明 2/3 以上投票者必须同意,且董事长必须同意;规则(3)说明多数投票者同意机制;规则(4)说明根据投票者具有的权重进行投票。

图 5 的程序说明 WT-Logic 能表示传统逻辑语言无法表达的复杂投票授权机制。

6 与相关逻辑语言的对比分析

表 2 列出了 WT-Logic 与相关逻辑语言的对比分析。

表 2 与相关逻辑语言的对比分析

	非负 Datalog	Active-U-Datalog	Transaction Logic	Prolog	WT-Logic
更新原子		✓		✓	✓
执行顺序					✓
事务			✓		✓
谓词权重					✓
可选谓词					✓
多方投票					✓
推理的确定性 (可评价性)	✓	✓			✓

除了 WT-Logic 以外,所有语言均不具有表达谓词权重、可选谓词、多方投票、执行顺序等概念。WT-Logic 也具有推理的确定性,因而在表达 workflow 授权、多方授权等信息安全领域,WT-Logic 确实具有独特的优势。

结束语 本文针对 Datalog 语言缺乏表达事务和多方决策模型的能力,对 Datalog 进行了扩展,提出了带权重谓词的可选事务逻辑 WT-Logic,并对 WT-Logic 的语法、语义进行了说明,解释了其评价方法。最后,对 WT-Logic 语言在工作流授权和多方投票机制中的应用进行了描述和举例,说明了 WT-Logic 的表达力和可应用性。

下一步,将对 WT-Logic 在社交网络多方授权模型中的应用进行具体研究。

参考文献

- [1] Vera Z M, Julia S, Serge A, et al. Collaborative Access Control in WebdamLog[C]//Proceeding of the ACM Sigmod Conference on Data Management, 2015. Melbourne, Australia, 2015: 197-211
- [2] Liu X, Alechina N, Logan B. Expressing User Access Authorization Exceptions in Conventional Role-Based Access Control[C]//International Conference on Information Security Practice and Experience, 2013: 233-247
- [3] Galland A. Distributed data management with access control; social Networks and Data of the Web[J]. Nature Communications, 2011, 5: 4864
- [4] Zhong Yong, Qin Xiao-lin, Liu Feng-yu. Obligation Authorization Model and Its Implementation Framework for DRM[J]. Journal of Software, 2010, 21(8): 2059-2069 (in Chinese)
钟勇, 秦小麟, 刘凤玉. 一种面向 DRM 的责任授权模型及其实施框架, 软件学报, 2010, 21(8): 2059-2069
- [5] Zhong Yong, Zhang Hong, Liu Feng-yu, et al. A Digital Rights

Management Mechanism and Implementation Based on Logic Framework[J]. Journal of Computer Research and Development, 2010, 47(2): 223-230 (in Chinese)

钟勇, 张宏, 刘凤玉, 等. 一种基于逻辑框架的数字版权管理机制和实现[J]. 计算机研究与发展, 2010, 47(2): 223-230

- [6] Hu H, Ahn G J, Jorgensen J. Multiparty Access Control for Online Social Networks: Model and Mechanisms[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(7): 1614-1627
- [7] Amrutha P, Sathiyaraj R. Privacy Management of Multi User Environment in Online Social Networks (OSNs)[J]. GJCST-E: Network, Web & Security, 2013, 13(10)
- [8] Bessedra R, Kifer M. Planning with Regression Analysis in Transaction Logic, Web Reasoning and Rule Systems [M]. Springer International Publishing, 2015: 45-60
- [9] Bessedra R, Kifer M. State Space Planning Using Transaction Logic[M]. Practical Aspects of Declarative Languages, Springer International Publishing, 2015: 17-33
- [10] Montesi D, Bertino E, Martelli M. Transactions and updates in deductive databases[J]. IEEE Trans. Knowl. Data Eng., 1997, 9(5): 784-797
- [11] Bertino E, Catania B, Gori R. Active-U-Datalog: integrating active rules in a logical update language[C]//Proc. of International Seminar on Logic Databases and the Meaning of Change, Schloss Dagstuhl, Germany, 1998: 107-133
- [12] Tom J A, Bas K, Frank N, et al. Datalog Queries Distributing over Components[C]//Proc. of 18th International Conference on Database Theory (ICDT 2015). Dagstuhl, Germany, 2015: 308-323
- [13] Radhakrishnan D. Dynamics of Belief; Horn Knowledge Base and Database Updates[C]//Proc. of 38th Annual German Conference on AI(KI 2015), LNCS 9324. Dresden, Germany, 2015: 341-348

(上接第 144 页)

- [4] Rushby J. Noninterference, transitivity, and channel-control security policies[M]. SRI International, Computer Science Laboratory, 1992
- [5] Liu Wei-peng, Zhang Xing. Research of duality and multi-level security model based on intransitive noninterference theory[J]. Journal on Communications, 2009, 30(2): 52-58 (in Chinese)
刘威鹏, 张兴. 基于非传递无干扰理论的二元多级安全模型研究[J]. 通信学报, 2009, 30(2): 52-58
- [6] Chen Ju, Tan Liang. Trusted Terminal Model Based on Process Protection[J]. Computer Science, 2011, 38(4): 115-117 (in Chinese)
陈菊, 谭良. 一个基于进程保护的可信终端模型[J]. 计算机科学, 2011, 38(4): 115-117
- [7] Xu Fu. Intransitive Noninterference Trusted Model Supporting Process Codes Modification[J]. Computer Engineering, 2013, 39(11): 150-153, 168 (in Chinese)
徐甫. 支持进程代码修改的非传递无干扰可信模型[J]. 计算机工程, 2013, 39(11): 150-153, 168
- [8] Qin Xi, Chang Chao-wen, Shen Chang-xiang, et al. Research on Trusted Terminal Computer Model Tolerating Untrusted Components[J]. Chinese Journal of Electronics, 2011, 39(4): 934-939 (in Chinese)

秦晰, 常朝稳, 沈昌祥, 等. 容忍非信任组件的可信终端模型研究[J]. 电子学报, 2011, 39(4): 934-939

- [9] Goguen J A, Meseguer J. EQLOG: Equality, types, and generic Modules for logic programming[M]. Functional and Logic Programming. DeGroot D, Lindstrom G. eds., Springer-Verlag, 1986
- [10] 梁元. 基于云计算环境下的可信平台设计[D]. 成都: 电子科技大学, 2013
- [11] Zhu C, Dai X. Model of trust management based on finite state machine[C]//2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE, 2012: 161-164
- [12] Si Li-min, Cai Mian, Chen Yin-jing, et al. Research of a Trust Chain Transfer Model[J]. Computer Science, 2011, 38(9): 79-81 (in Chinese)
司丽敏, 蔡勉, 陈银镜, 等. 一种信任链传递模型研究[J]. 计算机科学, 2011, 38(9): 79-81
- [13] Zhang Xing, Huang Qiang, Shen Chang-xiang. A Formal Method Based on Noninterference for Analyzing Trust Chain of Trusted Computing Platform[J]. Chinese Journal of Computers, 2010, 33(1): 74-81 (in Chinese)
张兴, 黄强, 沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 计算机学报, 2010, 33(1): 74-81