《智能信息处理》课程作业

三元形式概念分析的 RBAC 访问控制设计

吴敌

作业	分数[20]
得分	

2021 年 11 月 27 日

三元形式概念分析的 RBAC 访问控制设计

吴敌

（大连海事大学 信息科学技术学院，辽宁 大连 116026）

摘 要:形式概念分析可以用于设计访问控制所需要的层次结构，文献中提及的方法通常是将三维访问控制矩阵转换成二元形式背景，进行这种转换主要目的是导出形式概念、概念格结构以及角色层次和 RBAC 的约束。为了探索三元形式概念分析在 RBAC 访问控制中的应用，提出了三元形式概念分析对 RBAC 进行建模的方法，不必将三维访问控制矩阵转换为二元形式背景即能实现角色层次和角色责任分离。实验部分以医疗系统网络为例展示了该方法遵循 RBAC 角色层次和角色责任分离约束，证明了三元形式概念分析可对 RBAC 访问控制策略提供合理的表示。

关键词: 访问控制; 概念格; 基于角色的访问控制; 角色层次

中图法分类号 TP309

Design of Role Based Access Control for Triadic Concept Analysis

Wudi

(School of Information Science and Technology, Dalian Maritime University, Dalian 116026，China)

Abstract: Formal concept analysis can be used to design access control hierarchy．There are investigations reported in the literature so far on the logic that transforms the three dimensional access control matrix into dyadic formal contexts． The transformation is mainly to derive the formal concepts， lattice structure and implications to represent the role hierarchy and constraints of RBAC． In order to explore the application of triadic concept analysis in RBAC access control，we have represented RBAC three dimensional matrix as triadic lattice structure achieving role hierarchy and separation of duty constraints without transforming the triadic context into dyadic formal contexts． The experimental analysis show that triadic FCA can provide a suitable representation of RBAC policy and demonstrate how this representation follows role hierarchy and constraints of RBAC on sample healthcare network．

Key words: access control; concept lattice; role based access control; role hierarchy

0 引 言

访问控制是重要的安全机制之一，访问控制系统能够根据访问控制策略中指定的访问权限设置和控制用户的访问权限。其中基于角色的访问控制(RBAC) 以其强大的功能适用于多种类型用户的需求，除了在企业系统中广泛应用之外，RBAC 也在诸如类 UNIX 操作系统和数据库管理系统中实现。RBAC 的主要优势在于它是策略中立的，通过角色的层次结构和约束条件，可以表达广泛的安全策略［1］。RBAC 最初由 Sandhu 于 1996 年提出［2］，随后由 NIST 标准化［3］，RBAC 在主体和权限之间引入角色的概念，通过对角色的授权来控制主体对资源的访问。用户可以执行分配给其对应角色的访问权限。角色将每个用户映射到一组权限。RBAC 模型支持 3 个安全原则: 数据抽象，最小权限和角色责任分离。NIST 标准将 RBAC 划分为核心 RBAC，层次 RBAC 和限制 RBAC［3］。核心 RBAC 包含 RBAC 的基本功能。层次 RBAC 除了核心 RBAC 功能外，还遵循角色层次访问结构。限制 RBAC 遵循角色责任分离(SoD)等约束［4］。文［5］对 RBAC 进行了深入讨论并提出了几种对 RBAC 建模的方法。由于 RBAC 在诸多文献中已得到充分的讨论，本文对于 RBAC 的基础将不再赘述。

形式概念分析(FCA)是一种基于格理论的数学框架，主要用于知识的表示、提取和分析［6－7］。形式概念分析的基础是形式背景，定义为(G，M，Y) ，其中 G 是对象集合，M 是属性集合，Y 是这两个集合之间的二元关系。这种结构也被称为二元形式背景。文［8－10］提出了采用形式概念分析对 RBAC 建模的方法。RBAC 访问控制矩阵是由角色(R)，数据对象(D)和权限(P)表示的三维矩阵，在形式概念分析中访问控制矩阵可以确定一个描述 RBAC 这 3 个部分之间的关系三元形式背景。应用形式概念分析的过程中，在对二元形式背景进行转换的基础上，采用形式概念分析算法进行概念格构造、属性探索和含义分析，以便推导 RBAC 的角色层次结构和职责分离约束，这种转换通过将三元形式背景中的任意两个元素的向量积作为二元形式背景的对象，将另外一个元素作为属性实现的。例如，将三元形式背景(R，D，P，Y) 转换为二元情形(R×D，P，YR×D，P) 。然而，从二元情形的基本概念出发，形式概念分析被扩展到三元情形，其中输入数据将是在称为三元形式背景的表中表示的三维关系数据［11］。表中的条目表示哪些对象具有哪些属性。这种表示类似于 RBAC 三维数据。但现有文献中没有采用三元形式概念分析直接处理三元形式背景而不将其转化为二元形式背景的研究。基于已有的研究成果，我们将形式概念分析从二元推广到三元，在三元形式概念分析中，输入数据是三维关系数据，可以表示为三元形式背景［12］。将形式概念分析应用于 RBAC 建模时，在满足 RBAC 的角色层次结构和角色职责分离约束的情况下，三元形式概念分析能够合理表示 RBAC 访问控制策略，也更具应用前景。

综上所述，本文提出了以下 3 个问题: 如何用三元形式概念分析如何对 RBAC 进行合理的表示; 如何理解和解释三维 RBAC 矩阵产生的三元层次概念格; 这种表示是否遵循策略约束和隐含权限; 本文在不改变 RBAC 三元背景的前提下，通过三元形式概念和三元概念格对 RBAC 进行建模。

1 相关研究

在一些涉及到形式概念分析的文献中，已经将形式概念分析的二元算法推广到三元形式背景当中［13－14］。文［15］讨论了三元形式概念分析在在认知系统模型中的应用，文［16］讨论了三元形式概念分析和三元聚类，文［17］使用形式概念分析建模 RBAC，并实现了角色层次结构。文［18］提出了一种利用形式概念分析设计 RBAC 的方法。文［19］提出了基于模糊形式概念分析的模糊角色访问控制模型。这些研究都使用了二元形式概念分析。

2 相关知识

2.1 二元形式概念分析

定义 1 (形式背景) 一个形式背景 K： =(G，M，I) 是由两个集合 G 和 M 以及 G 与 M 间的关系 I 组成。G 的元素称为(形式) 对象，M 的元素称为(形式) 属性。(g，m) ∈I 或 gIm 表示对象 g 具有属性 m。

定义 2 设 A 是对象集合 G 的一个子集，我们定义 f(A)：= { m∈M | ∀g∈A，gIm} (具有 A 中对象共同属性的集合)

相应地设 B 是对象集合 M 的一个子集，我们定义 g(B)：= { g∈G |∀m∈B，gIm} (具有 B 中对象共同属性的集合)

定义 3 (形式概念) 形式背景 K：=(G，M，I) 上的一个形式概念是二元组(A，B)，有 A↑= B，B↓= A，我们称 A 是概念(A，B) 的外延，B 是(A，B)的内涵。B(G，M，I)表示背景(G，M，I)上的所有概念的集合。

定义 4 (概念格) 若(A1，B1)，(A2，B2)是某个背景上的两个概念，而且 A1⊆A2，则我们称(A1，B1)是(A2，B2) 的子概念，(A2，B2)是(A1，B1) 的超概念，记作(A1，B1) ≤(A2，B2)，关系≤称为是概念的“层次序”，(简称“序”)。(G，M，I)的所有概念用这种序组成的集合用 B(G，M，I) 表示，称它为背景(G，M，I)上的概念格。

2.2 三值背景

定义 5 (多值背景) 一个多值背景 K： =(G，M，W，I)是由集合 G，M，W 及它们之间的一个三元关系 I(即 IG×M×W)组成，且下式成立:

$$(g, m, w) \in I \text{ 及 } I \Rightarrow w = v \qquad (1)$$

G 的元素称为对象，M 的元素称为(多值)属性，W 的元素称为属性的值。属性 m 的域定义为 dom(m)：= { g∈G | (g，m，w) ∈I，w∈W}，如果 dom (m) = G，则称 m 是完全的。如果一个多值背景的所有属性都是完全的，则称这个多值背景是完全的。

定义 6 (三值概念) 三元背景(G，M，W，I) 的三元概念被定义为 1 个三元组(A1，A2，A3)，其中 A1⊆G，A2⊆M，A3⊆W 分别满足条件 A1×A2×A3⊆I。这个定义是从二元形式概念的定义到三元形式概念情况下的推广。A1，A2，A3 分别被称为概念(A1，A2，A3)的外延、内涵和方法。考虑一个三元背景 K：=(X1，X2，X3，I)，我们由此定义可以建立 3 个二元形式背景:

$$K^{(1)}=(X1, X2\times X3, I^{(1)}) \quad (2)$$

$$K^{(2)}=(X2, X1\times X3, I^{(2)}) \quad (3)$$

$$K^{(3)}=(X3, X1\times X2, I^{(3)}) \quad (4)$$

其中 $x_1 I^{(1)}(x2, x3) :\Leftrightarrow x_2 I^{(2)}(x1, x3) :\Leftrightarrow x_3 I^{(3)}(x1, x2)$ 。

2.3 三元形式概念分析

定义 7 (三元形式概念运算外导运算) 对于{ (j＜k)，{ i，j，k} = { 1，2，3}，Z⊆X_i}和 Z⊆X_i 且 Y⊆$X_j\times X_k$，外导运算符$(-)^i$定义如下:

$$\Psi: Z\rightarrow Z^{(i)}: \left\{ \begin{matrix} (x_i, x_k)\in X_j\times X_k \mid \\ (X_i, X_j, X_k)\in I \forall x_i\in Z \end{matrix} \right\} \quad (5)$$

$$\Psi': Y\rightarrow Y^{(i)}: \left\{ \begin{matrix} x_i\in X_i \mid (x_i, x_j, x_k)\in I \\ \forall (x_j, x_k)\in Y \end{matrix} \right\} \quad (6)$$

对于{ i，j，k} = { 1，2，3}，外导运算产生上述 3 个二元形式背景 $K^{(1)}$，$K^{(2)}$，$K^{(3)}$，即 $K^{(i)}=(X_i, X_j\times X_k, I^{(i)})$当{ i，j，k} = { 1，2，3}。

定义 8 (三元形式概念运算内导运算) 对于{ i，j，k} = { 1，2，3}，$Z_i\subseteq X_i$，$Z_j\subseteq X_j$，$Z_k\subseteq X_k$，(i，j，Z_k)内导运算定义为:

$$\Phi: Z_i\rightarrow Z_i^{(i,j,Z_k)}: \left\{ \begin{matrix} x_j\in X_j \mid (x_i, x_j, x_k)\in I \\ \forall (x_i, x_k)\in X_i\times X_k \end{matrix} \right\} \quad (7)$$

$$\Phi': Z_j\rightarrow Z_i^{(i,j,Z_k)}: \left\{ \begin{matrix} x_i\in X_i \mid (x_i, x_j, x_k)\in I \\ \forall (x_j, x_k)\in X_j\times X_k \end{matrix} \right\} \quad (8)$$

内导运算导出背景 $K_{Xk}^{i,j}$：=(X_i，X_j，$I_{Xk}^{i,j}$)，其中(x_i，x_k)∈$I_{Xk}^{i,j}$，当且仅当(x_i，x_j，x_k)∈I∀x_k∈X_k。(x_i，x_k)∈$I_{Xk}^{i,j}$称为对象 x_i 在 x_k，其中 x_k∈X_k 的所有条件下具有属性 x_i。Ψ和Ψ'称为外导运算，两者构成外闭包。类似的，Φ和Φ'称为内导运算，它们构成内闭包。因此，为了在 Z_1 的外延生成一个三元概念，第一步将在背景 $K_{A3}^{1,2}$上生成一个二元概念。进而，三元概念通过在 $K^{(3)}$中相应的运算 $K_{A3}^{1,2}$而获得。

定义 9 (三元概念形成) 一个外延中包含 Z_1 的概念定义为($Z^{(1,2,X3)(1,2,X3)}$，$Z_1^{(1,2,X3)}$，($Z_1^{(1,2,X3)(1,2,X3)}\times Z_1^{(1,2,X3)}$) $^{(3)}$)。该形成过程首先确定非空对象的集合 Z_1。然后找到 Z_1 中所有对象在 X_3 给出的所有条件下的属性集合。最后将 Z_1 推广到在 X_3 的所有条件下具有这些属性的所有对象的集合。

定义 10 (三元概念格) 对于 i∈{1，2，3}，存在一个层次序$\leqslant_i$和由(A1，A2，A3) $\leqslant_i$(B1，B2，B3)：⇔$A_i\subseteq B_i$ 和 (A1，A2，A3)～$_i$(B1，B2，B3)：⇔$A_i=B_i$(i = 1，2，3) 定义的相应的等价关系～$_i$。以这种序组成的集合称为三元概念格。

三元概念格是一种对称结构，其中的对象集，属性集和条件是等价的。一般地，我们将这种结构绘制为三角形图。为方便理解，可为每个外延，内涵和形式绘制完整的概念格。

3 提出的方法

为了实现三元形式概念分析对 RBAC 模型进行表示，利用上面定义的外闭包运算和内闭包算，给出了将三维访问控制矩阵导出三元概念的方法:

1) 确定给定访问策略的角色(R)，数据对象(D)和访问权限(P)。

2) 将具有角色(R)、数据对象(D)和访问权限(P)的三维访问矩阵构成三元形式背景: $K_{R, D, P}$：=(R，D，P，I)，其中 I 表示 R，D 和 P 的三元关系。

3) 对于每个权限集合 H⊆P，使用内闭包运算Φ和Φ'计算二元背景(R，D × H，Y^3)。

4) 使用文［20］中的二元概念生成算法，计算步骤 3 中生成的背景中的每一个概念。

5) 对于每个二元概念，使用外闭包运算 Ψ 和Ψ'计算包含它的条件集合。

6) 形成定义 9 给出的三元概念。

7) 对于所有子条件集合重复步骤 5) 。

8) 若存在多余的三元概念则将其删除。

利用上述方法，我们从三维 RBAC 矩阵导出三元概念，得到三元形式概念分析的 RBAC 模型表示。算法上这个过程复杂度为指数阶。为了说明问题，考虑表 1 所示的 RBAC 三元背景(R，D，P，Y)。形式背景中包含 4 个角色，3 个数据对象和 3 个权限。

表 1 RABC 三元形式背景

Tab.1 RABC triadic context

R	P_1			P_2			P_3		
	d_1	d_2	d_3	d_1	d_2	d_3	d_1	d_2	d_3
r_1			×	×	×	×	×		
r_2	×	×	×	×	×		×		
r_3		×	×	×	×	×	×	×	×
r_4		×			×	×		×	×

考虑{ i，j，k} = { 1，2，3}，$X_1=RA_3=\{p_1，p_2\}$ 且 Z={ r_3}。根据定义 8 中内导运算可得到Φ(Z)=(d_2，d_3)和Φ'Φ(Z) = (r_2，r_3)。此外，由定义 7 的外导运算可得到Ψ(Z) = { (d_2，p_1) ，(d_3，p_1)，(d_2，p_2)，(d_3，p_2)，(d_2，p_3)，(d_3，p_3) }。其中注意到Ψ'(\Ψ(Z)) = (r_3，r_4)\。根据定义 9 可得到三元概念({ r_3，r_4} ，{ d_2，d_3} ，{ p_1，p_2，p_3})。

4 结 论

本文提出的方法将三维 RBAC 矩阵表示为三元概念格，即可实现角色层次和职责分离。给出了三维 RBAC 矩阵生成三元概念格的层次解释，从三元背景中推导条件属性含义，证明了 RBAC 元素之间的依赖关系。方法为使用三元形式概念分析表示 RBAC 策略提供了理论基础，可以在访问控制系统中得到应用。

参 考 文 献

[1] HUANG H，SHANG F，LIU J． Handling Least Privilege Problem and Role Mining in RBAC［J］． Journal of Combinatorial Optimization 2013，30(1) : 1．

[2] SANDHU R． Role Hierarchies and Constraints for Lattice-based Access Controls［C］/ / European Symposium on Research in Computer Security． Rome: Springer Berlin Heidelberg， 1996， 1146: 65．

[3] SANDHU R，FERRAIOLOD，KUHN R． The NIST Model for Role-based Access Control: Towards a Unified Standard［C］/ /ACM Workshop on Role-based Access Control． Berlin: ACM Dig ital Library，2000: 47．

[4] KUGBLENU F M，ASIM M． Separation of Duty in Role Based Access Control System: A Case Study［D］． Sweden: Blekinge Institute of Technology，2007．

[5] FADHEL A B，BIANCULLI D，BRIAND L．A Comprehensive Modeling Framework for Role-based Access Control Policies［J］． Journal of Systems and Software，2015，107: 110．

[6] POELMANS J，KUZNETSOV S O，IGNATOV D I，DEDENE G．Formal Concept Analysis in Knowledge Processing: A Survey on Models and Techniques［J］．Expert Systems with Applications，2013，40(16) : 6601．

[7] KUMARC A，S R INIVAS S．Concept Lattice Reduction Using Fuzzy K-Means Clustering ［J］． Expert Systems with Applications，2010，37(3) : 2696．

[8] KNECHTEL M． Access Restrictions to and with Description Logic Web Ontologies ［ D ］． Dresden: Technische Universitt Dresden，2011．

[9] SELLAMIM，GAMMOUDIMM，HACIM S．Secure Data Integration: A Formal Concept Analysis Based Approach［C］/ / Intel Conference on Database and Expert SystemsApplications．Munich: Springer International Publishing，2014，8645: 326．

[10] HAN Daojun，ZHUO Hankui，XIA Lanting，et al． Permission and Role Automatic Assigning of User in Role-based Access Control［J］． Journal of Central South University，2012，19(04) : 1049．