面向射孔数据协作的文件授权访问控制模型

尚福华,李 盼
(东北石油大学 计算机与信息技术学院,黑龙江 大庆 163318)

摘 要:适当的访问控制机制是支持协作系统正常运行的一项关键技术。建立适当的授权策略在协作系统中是有困难的,往往将传统的授权机制模型应用在协作系统中,不能为多用户之间提供足够的支持。针对射孔校深数据协同处理平台,结合射孔数据协同处理的动态过程,提出一种支持协作的文件授权访问控制模型,使其更适合于协同工作环境的访问控制。重点分析了多用户之间的动态授权机制,采用文件信任评价机制保证权限文件的安全性,基于 Hash-索引数据库,保证权限文件在协作系统中的唯一性。介绍了文件授权访问控制模型各组件的构成及具体应用。在该模型中,用户权限值会随着其他多个用户授权而动态变化,用户能够通过对权限文件进行信任评价来防止恶意分享文件,获取其权限。

关键词:协同环境;动态授权;文件共享;访问控制
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2016)09-0119-05
doi:10.3969/j.issn.1673-629X.2016.09.027

File Authorization Access Control Model for Perforated Data Collaboration

SHANG Fu-hua, LI Pan
(School of Computer and Information Technology, Northeast Petroleum University, Daqing 163318, China)

Abstract: Appropriate access control mechanism is a key technology to support the normal operation of the collaborative work system. Construction of the appropriate authorization mechanism is very challenging for the cooperative system. The traditional access control system applied to the direct cooperation model is not enough for collaboration support among multiple users. In view of the dynamic process of the deep data processing platform and the collaborative process of perforating data, a file authorization access control model is proposed which supports collaboration, to make it more suitable for access control in collaborative work environment. It focuses on the analysis of the dynamic authorization mechanism between multi users in this paper, using the file trust evaluation mechanism to ensure the security of access files. Based on the Hash-index database, the uniqueness of the document in the collaborative system is ensured. The structure of file access control model and its application is introduced. In this model, the user rights value will change with other users' behavior, and users can use the authority file to prevent malicious sharing files and access permissions.

Key words: collaborative environment; dynamic authorization; file sharing; access control

1 概 述

利用射孔方法以达到最后完井的目的,是当今世界各国开发油田的主要手段。射孔的关键是把射孔枪准确送到目的层段,将顶部第一发弹对准目的层顶界,习惯上把这项对射孔层点火深度进行准确定位的工作称为射孔校深[1]。

精准地定位到射孔枪的深度位置是射孔施工的关键。射孔深度计算工作决定着射孔的精度及准确性。对射孔深度数据处理的主要工序进行分析,其处理过程包括资料接收、任务下达、过程审核、技术支持等相关工作,优化工作流程,提高射孔作业系统的工作效率和程度。进行有效的信息共享互换,实现业务信息的流转控制、工序操作的流程控制、疑难井处理和问题资料返工的流程控制。由于射孔深度数据处理过程本身是一个动态过程,具有多部门和人员协同工作、动态性、临时性的特点,是保证处理结果的准确性和有效性的重要基础。但在应用新技术的同时,信息安全问题也越来越受到关注。

收稿日期:2015-12-13 **修回日期**:2016-04-06 **网络出版时间**:2016-08-01
基金项目:国家自然科学基金资助项目(61170132);国家重大专项(2011ZX05020-007)
作者简介:尚福华(1962-),男,教授,博士(后),研究方向为人工智能、数据挖掘、计算机理论与方法;李 盼(1990-),男,硕士研究生,研究方向为计算机应用技术。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160801.0907.058.html

文献[2]归纳了常见的访问控制机制,包括强制访问控制(Mandatory Access Control,MAC)、自主访问控制(Discretionary Access Control,DAC)以及在 MAC 和 DAC 的基础上提出的基于角色的访问控制(Role-Based Access Control,RBAC)。

通过多用户的合作,一起来实现某项任务或者工作的目标是协同环境的特性之一。协同环境中,把握协同和安全之间的尺度是十分困难的。由于在协同环境中对有需求的用户来说,可以共享资源、信息甚至可以是其他用户,但是安全是达到资源的保密的目的以及能够保证其完整性和可用性,进而保证只能得到授权的用户才能共享到相应的资源、信息甚至其他用户的协作[3]。

对于协作系统的特殊性,提出了对协作提供支持的访问模型:基于任务的访问控制(Task-Based Access Controls,TBAC)[4]。在 TBAC 中,主被动的安全模型的概念被首次提出。被动安全模型就是在传统的访问控制模型中,以主体、客体为核心,但是控制策略是静态的,主体访问客体的权限机制与上下文是没有关系的。同时与之相对应的主动安全模型是指保证安全以及建模的安全性是靠着活动或者任务为核心的机制,安全动态地管理任务的执行过程,这样主体访问客体的权限是根据任务的上下文来变化的。TBAC 是解决协作环境中访问控制的新思路。

针对 TBAC 和 RBAC[5] 整合在一起的基于角色-任务的访问控制(Task-Role Based Access Control,T-RBAC)[6]、基于组的访问控制模型(Team-Based Access Control,TMAC)[4],Georgiadis 等[7] 在 TMAC 的基础上进行完善,提出将 TMAC 的思路集成到 RBAC[5] 中的一个中间件;翟治年[8] 对企业中的协作环境的访问控制模型进行了研究;Bijon 等[9] 提出多级系统中以组为中心的访问控制模型;闫玺玺等[10] 研究了一种在共享环境下对敏感数据的访问控制机制;姚志强等[11] 提出一种在协作环境下的基于信任的访问控制机制。上述模型都对协作环境下访问控制的新需求做了研究。於光灿把能够支持协作的访问控制机制分为了两类:通用型访问控制模型和协作型访问控制模型。在通用型访问控制模型里模型与协作相关的元素没有关系,是系统的应用层来实现的;协作型访问控制模型中涉及与协作相关的问题,直接对用户间的协作提供了支持[12]。

文中以射孔数据协作为基础,设计了一种面向射孔数据协作的文件授权访问控制模型,使用户权限值随其他用户行为动态变化。该模型支持文件信任评价,结合 Hash-索引数据库,有效避免了对权限文件恶意地分享**万方数据**

2 射孔数据协作流程对访问控制的需求

在射孔协作环境中,需要计算组内部、计算组之间或计算员与计算员之间相互协调与配合,来完成为射孔作业提供数据支持这一任务。下面以射孔深度协同处理为例,说明在协作环境中对访问控制的安全需要。射孔深度数据处理分为两个部分,由计算组 1 和计算组 2 分别计算,然后提交进行计算生成报表。计算组成员所涉及的节点任务如图 1 所示。

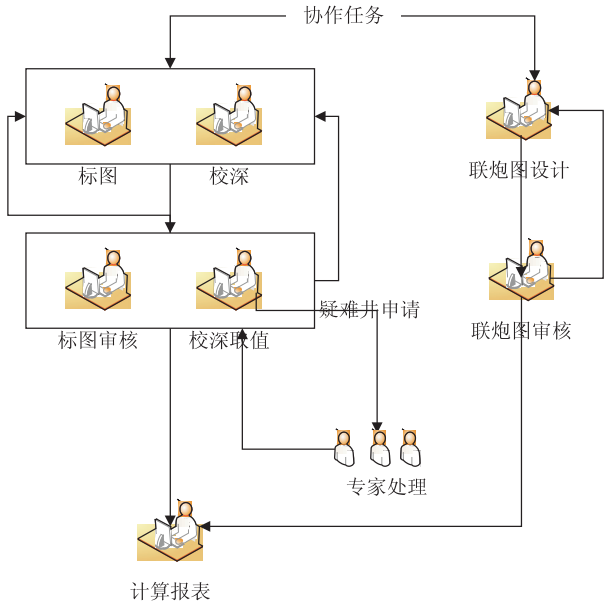

图 1 射孔数据协作的部分流程

上述协作流程的访问控制需求如下:

(1)计算组 1 的所有成员有标图计算成员 B_1、标图审核成员 A_1,校深计算员 B_2、校深审核员 A_2、疑难井专家 C_2。由于企业内部人员变动及疑难井问题出现的不同,可以有 A_1、A_2 分别动态地对 B_1、B_2、C_2 授权进行处理。

(2)计算组 2 的所有成员有联炮图设计成员 B_3、联炮图审核员 A_3,同样 A_3 可以动态地对 B_1 授权处理。

依照该例中的需要,制定访问控制目标:

(1)计算员参与协作任务时,同协作组内的用户动态授权实现对资源的共享以及数据的双向流动;

(2)在执行协作任务时用户设定的即时权限及撤销不能使权限滥用;

(3)对权限文件使用信任评价机制来防止权限文件的恶意分享。

3 射孔数据协作文件授权访问控制模型的描述

3.1 射孔数据协作文件授权访问控制模型的基本原理

射孔数据协作文件授权访问控制模型描述:该模

型是针对传统的访问控制模型,提出了多计算员之间的动态授权以及对权限文件信任评价模式,也就是说在模型中任意一个计算员都设置有一个初始的权限值,权限值会由其他多个计算员对其授权发生改变;权限文件有其发布者设置其可用阈值,通过信任评价机制来保证权限文件是否安全。任意一个计算员获取权限是通过能够访问到一个权限文件的,但是得保证到该用户的权限值大于或等于其权限文件的阈值。

符号说明如表 1 所示。

表 1　符号说明

符号	含义
A	表示任意一个计算员能够发布和获取到权限文件的权限
U_A	计算员 A 的权限值
p	表示权限文件
U_p^{init}	文件 p 的初始可用阈值

射孔数据协作文件授权访问控制模型中,计算员的权限值以及权限文件可用阈值的信任评价如下:

1)用户之间授权。

计算员 A 对计算员 B 进行授权时,计算员 B 的权限值会根据计算员 A 自身的权限值进行重新计算,更新计算员 B 的权限值(计算员 A 对计算员 B 授权,只提升 B 的权限值。避免计算员之间的权限值无限增长下去,系统规定被授权计算员的权限值不大于授权计算员,且是单项的、能够撤销的)。A 与 B 的权限值换算公式为:

$$U_B = U_B + U_A * f, 0 < f < 1 \quad (1)$$

其中,f 为关系系数。

关系系数是根据权限文件阈值分为几个等级及用户的权限值来确定,根据排列组合的思想可以将 f 定义为(0.1,0.2,0.5)。这样根据用户量来有效选定 f,通过不同的排列组合可以使用户的权限值通过授权达到权限文件的解锁阈值。

2)权限文件信任评价。

权限文件在被计算员发布到系统时,对已存在模型中的权限文件,该模型不能对其进行重复的存储操作,而是由计算员对使用过的权限文件进行信任评价并统计信任评价中正面及负面评价次数以及设定信任等级。设 T 为信任等级因子($T \in [-1,1]$),对 $T \in [-1,0]$,设定[-0.3,0]为轻微,并记录其评价时间和次数,[-1,-0.3]为不信任。

3)Hash 函数。

Hash 函数即为哈希函数,也可称为散列函数。其输入任意长度的信息,并通过其算法,进而压缩成固定长度并输出,其输出值被称为消息摘要或散列值。简而言之,应用到模型中就是将权限文件经过哈希计算得到固定长度且唯一的值[13-14]。

基于对权限文件的唯一性、安全性的考虑,将 Hash 函数应用到实际中,必要的规定如下:

(1)哈希函数可应用于任意大小的数据块。

(2)哈希函数可输出固定长度的值。

(3)很容易计算出对任意给定 p 的 $H(p)$。

(4)其满足单向性即唯一性,对任意的散列值 h,找到满足 $H(x) = h$ 的 p 是不可行的。

(5)其满足抗弱碰撞性,对给定的 p_1,只要 $p_1 \neq p$,存在 $H(p) = H(p_1)$ 是不可行的。

(6)其满足抗强碰撞性,对任意能够满足 $H(p) = H(p_1)$ 的偶对 $p_1 = p$ 在计算上是不可行的。

3.2　射孔数据协作文件授权访问控制模型的构成

射孔数据协作文件授权访问控制模型由 6 个模块组成,如图 2 所示。首先为用户分配初始权限值,设置用户权限值范围级别,规范化管理,避免权限值混乱,在射孔协同处理工作流程中依据最小特权原则对权限文件进行分级,规范化解锁阈值,避免其权限文件解锁阈值的混乱。计算员注册模块主要是在协作环境中增添了新的计算员。权限文件发布模块主要是将权限文件存储到权限文件的数据库中,特别注意该模块需先与哈希索引数据库进行相关信息判断。权限文件信任模块主要记录信任评价、信任等级以及正面或负面信任统计。获取权限模块主要是计算员获取权限,判定特定的计算员能否获取到权限。权限文件清除模块是与权限文件 Hash-索引数据库直接相连的,经过相关索引信息判断来清除权限文件。

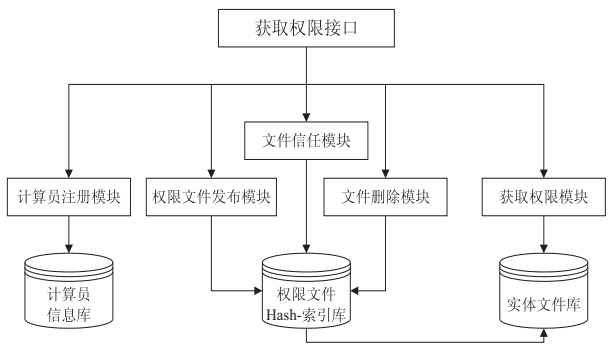

图 2　射孔数据协作文件授权访问控制模型的构成

另外,射孔数据协作文件授权访问控制模型中还包含实体文件库以及 Hash-索引库。其权限文件自身存储在实体文件库中,Hash-索引库存储着权限文件的索引、属性以及信任评级信息等。索引记录是链接到对应的权限文件,通过权限文件获取其权限。

4　具体应用

4.1　计算员注册模块

新的计算员是用此模块来注册的,详细情况如下:

(1)收集到计算员基本信息,录入到计算员数据库中。收集计算员属性的一个重要原因是确保射孔工作组中的每个计算员都有登录账号。信息表单根据数据库范式要求多表联合的方式,使每个属性字段长度能够符合编码要求。

(2)为计算员分配初始权限值。

4.2 权限文件发布模块

该模块是通过 Hash-索引数据库的对应索引信息判断是否重复存储,来完成权限文件的存储。Hash-索引数据库存储的是权限文件通过 Hash 函数的结果值、权限文件的索引信息以及信任评价等信息。权限文件发布过程如下:

1)计算员设定权限文件可用阈值 UF_p^{init} ,先不做其他操作。

2)经过 Hash 计算出权限文件的 $H(p)$,在 Hash-索引数据库检索查询 $H(p)$ 。

3)主要有两种情况:

(1)假如没有检索到 $H(p)$ 的记录,将 $H(p)$ 和 UF_p^{init} 存入 Hash-索引数据库,同时把权限文件存储到实体文件库中。设定的 UF_p^{init} 就是作为权限文件被获取到的可用阈值。值得注意的是,假如权限文件是计算员 B 发布的,那么可用阈值的取值 $UF_p \in (0, U_B)$ 。

(2)假如 $H(p)$ 被检索到,说明了权限文件在实体文件库中已被存储,那么就不能继续存储,同时根据信任评价信息情况来判断权限文件是否安全。假如都是正面的信任信息,那么说明此权限文件是安全的;假如信任等级因子 T 取负值,根据其对应所属区间,判断是轻微还是已经不被信任。如果是轻微等级,根据信任的评价时间及次数来判断是否通知其发布者(统计次数超过三次,且时间都是最近的,通知发布者是否清除更换)。如果不被信任,那么通知其发布者来说明此权限文件已不安全了,是否清除更换。

在图 3 中,权限文件发布模块将权限文件存储到实体文件库中,文件信任评价模块记录权限文件是否是被信任的来说明权限文件的安全性,判定权限文件是否被清除或被替换。

4.3 权限获取模块

该模块的关键是计算员之间的授权公式算法。详细的通过权限文件获取权限的过程:

(1)计算员 A 获取权限文件 p 的权限;

(2)获取计算员 A 的权限值 U_A 及可用权限文件可用阈值 UF_p ;

(3)通过比较 U_A 和 UF_p 的大小获取权限。

多计算员的动态授权体现在不同的任务时期,一个计算员的权限值会随着计算组或其他计算组的用户对其的授权行为而变化。变化过程如图 4 所示。

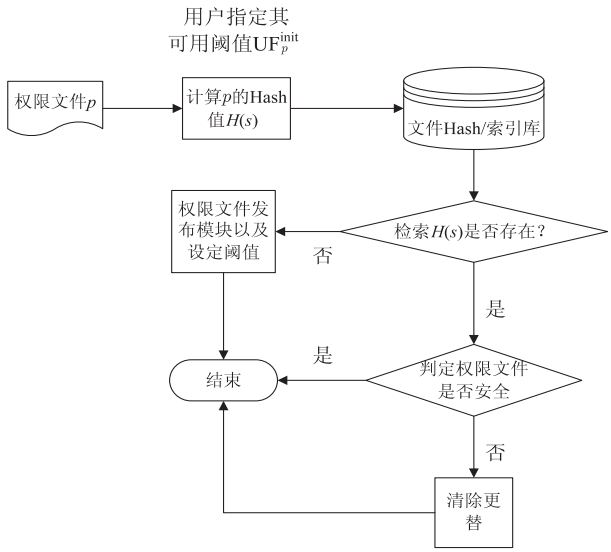

图 3 权限文件发布过程

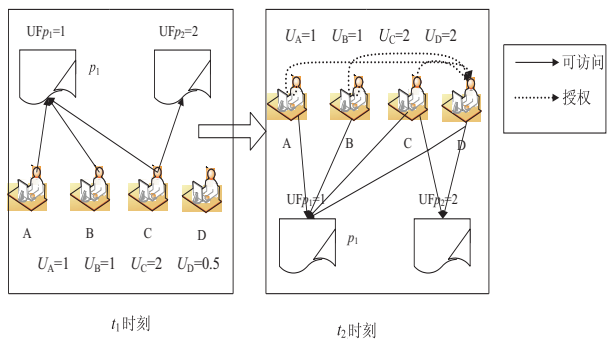

图 4 多用户授权过程

t_1 和 t_2 是系统中的任意两个任务时期。现假设权工作组计算员的系数 $f = 0.5$,则由式(1)得计算员 D 的权限值:

$U_D + U_A * 0.5 = 1.1$,此时 $U_D = U_A$,因此 $U_D = 1$;

$U_D = U_D + U_B * 0.5 = 1.5$,此时 $U_D > U_B$,因此 $U_D = U_B = 1$;

$U_D = U_D + U_C * 0.5 = 2$。

最后在权限文件 p_1 和 p_2 中获取权限。

4.4 权限文件删除模块

对于共同应用到某个权限的权限文件的所有计算员来说,删除其权限文件的过程为:

(1)权限最高的计算员删除权限文件的命令时,其他所有计算员对此权限文件的索引全部删除,或根据权限文件不安全的因素来删除权限文件。

(2)如果权限文件损坏或其他原因造成权限文件不可用,那么通过计算对应的权限文件索引表来处理:统计权限文件的索引个数,假如大于 0,权限文件被替换;假如为 0,权限文件从实体文件库中彻底清除,同时清除所有索引信息,不能被撤销。

具体过程如图 5 所示。

这样设计的目的可以确保权限文件的等级层次分明。

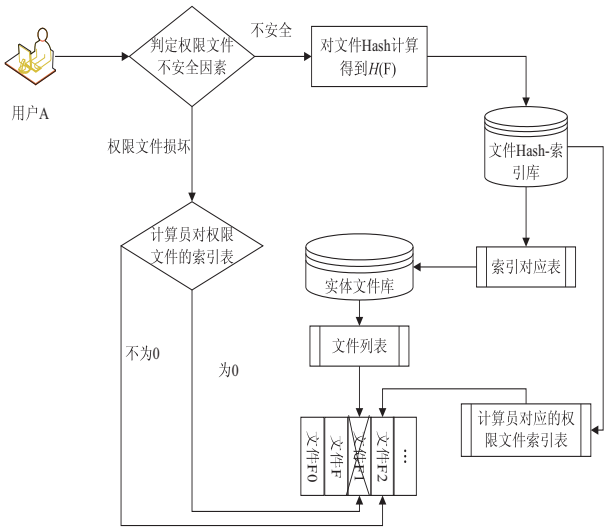

图 5　权限文件不安全因素的删除过程

5　结束语

文中以射孔数据协作为例,设计了支持协作环境下的文件授权访问机制,即多用户的动态授权机制和权限文件信任评价机制,并预防对权限文件的恶意再分享:

(1)在射孔数据协作文件授权访问控制模型中,计算员的权限值可以在其他计算员动态授权下增加,实现了动态授权管理;避免了只有管理员授权的局限性及专制权威,实现了多人授权的共同决策。该模型是通过访问权限文件控制模块的用户授权公式来体现多用户动态授权的。

(2)在协作任务中,用户可以对自己的任务设置相应的权限,通过权限文件的发布,可以使其他用户访问权限文件获取权限,动态实现任务的特殊授权及撤销。

(3)射孔数据协作文件授权访问控制模型通过计算员本身的权限值及信任评价来保证权限的可靠性授权,同时保证权限文件的安全性以及有效避免权限文件被破坏。另一方面,Hash-索引数据库能够保障权限文件在模型中的唯一性,而且避免了权限文件在恶意的分享时,减少权限高的权限文件转入到权限低的计算员的安全隐忧。同时,射孔数据协作文件授权访问控制模型具有如下特点:一个计算员得到同计算组的计算员或其他计算组的计算组的授权越多,其权限值就越高,但是不能高于授权计算员中最高的权限值,能够避免多个权限低的计算员将一个计算员的权限值授权的非常高,达到高权限的计算员;计算员之间的授权中,计算员的权限值越高,对其他计算员的权限值增长的越快。

参考文献:

[1] 倪德忠. 油气井射孔层位的深度定位方法[J]. 海洋石油,2004,24(2):88-92.

[2] 訾小超,张绍莲,茅　兵,等. 访问控制技术的研究和进展[J]. 计算机科学,2001,28(7):26-28.

[3] Thlone W,Ahn G J,Pai T,et al. Access control in collaborative systems[J]. ACM Computing Surveys,2005,37(1):29-41.

[4] Thomas R K,Sandhu R S. Task-based authorization controls (TBAC):a family of models for active and enterprise-oriented authorization management[C]//Proc of the IFIP WG11.3 workshop on database security. London: Chapman & Hal,1997:13-19.

[5] Sandhu R S,Coynek E J,Feinsteink H L,et al. Role-based access control models[J]. IEEE Computer,1996,29(2):38-47.

[6] Oh S,Park S. Task-role based access control (T-RBAC):an improved access control method for enterprise environment [C]//Proc of the 11th international conference on database and expert systems applications. Berlin:Springer,2000:264-273.

[7] Georgiadis C K,Mavridis I,Pangalos G,et al. Flexible team-based access control using contexts[C]//Proc of the ACM symp on access control models and technologies. New York: ACM,2001:21-27.

[8] 翟治年. 企业级协作环境中访问控制模型研究[D]. 广州:华南理工大学,2012.

[9] Bijon K Z,Sandhu R S,Krishnan R. A group-centric model for collaboration with expedient insiders in multilevel systems [C]//Proc of the 2012 international conference on collaboration technologies and systems. Piscataway, NJ: IEEE, 2012: 419-426.

[10] 闫玺玺,耿　涛. 面向敏感数据共享环境下的融合访问控制机制[J]. 通信学报,2014,35(8):71-77.

[11] 姚志强,熊金波,马建峰,等. 以社区域为中心基于信任的访问控制[J]. 通信学报,2013,34(9):1-9.

[12] 於光灿. 协作环境中访问控制模型研究[D]. 武汉:华中科技大学,2008.

[13] 郑　东,赵庆兰,张应辉. 密码学综述[J]. 西安邮电大学学报,2013,18(6):1-10.

[14] Kanso A,Yahyaoui H,Almulla M. Keyed Hash function based on a chaotic map[J]. Information Sciences,2012,186(1):249-264.