DOI:10.16644/j.cnki.cn33-1094/tp.2018.09.005

联盟环境下基于属性存取的跨域认证授权机制*

刘其群

(河南农业职业学院，河南 郑州 451450)

摘 要：在隐私得到保护的前提下，为了解决位于不同自治域的主体之间动态地交换数据和实现资源共享的问题，提出了一个基于属性的授权机制。该机制依赖于信任的第三方或联盟中心，对位于各组织中的主体和对象的属性进行映射，以属性集合作为主体的代表，确保不同组织的属性集合具有一致的存取权限。在本机制中给出了跨域属性映射的模型和服务策略，并结合模型给出其工作流程，实现跨安全域的身份验证并进行授权。

关键词：隐私；授权机制；联盟中心；属性映射；服务策略

中图分类号：TP309.2 **文献标志码**：A **文章编号**：1006-8228(2018)09-14-03

Cross-domain authentication and authorization mechanism based on attribute access in federated environment

Liu Qiqun

(*Henan Agricultural Vocational College, Zhengzhou, Henan 451450, China*)

Abstract: In order to solve the problem of being able to exchange data and share resources dynamically under the premise of protecting privacy between subjects located in different autonomous domains, an attribute-based authorization mechanism is proposed. The mechanism relies on a trusted third party or federation center to map the attributes of the principals and objects located in each organization, with the attribute set as the representative of the subjects, ensuring that the attribute sets of different organizations have consistent access rights. In this mechanism, the cross-domain attribute mapping model and the service strategy are given, and the workflow is given according to the model. Authentication and authorization about the cross-security domain are implemented.

Key words: privacy; authorization mechanism; federation center; attribute mapping; service strategy

0 引言

针对不同的应用环境，采用不同的访问控制策略，访问控制技术一直是信息领域的研究热点，主要包括自主访问控制DAC、强制访问控制MAC、基于角色的访问控制RBAC和基于任务的访问控制TBAC。

其中基于角色的访问控制RBAC，通过在用户和权限之间引入角色，将用户和角色联系起来，能够降低管理的复杂性和管理成本，通过对角色授权来控制用户对系统资源的访问[1-2]。RBAC目前在授权管理领域有较为广泛的应用，但存在着无法解决跨域多应用系统高效统一授权问题[3]。

为了解决跨域应用系统的授权问题，我们基于RBAC原理，结合基于属性的访问控制[4]，给出了联盟环境下基于属性存取的跨域认证授权机制。该机制在基于用户角色的基础上，根据主体所拥有的属性及与当前策略相关的环境条件，实现对访问者进行统一授权控制的策略。

1 架构设计

1.1 总体架构

联盟环境下基于属性存取的跨域认证授权机制涉及到多个自治域，每个自治域有各自的用户、资源和属性，能够对域内用户进行独立的认证和授权，系统总体架构如图1所示。其中D_0代表认证授权机制的

收稿日期：2018-06-19

*基金项目：河南省郑州市科技局科技攻关项目"跨域认证授权机制的研究"(20150279)

作者简介：刘其群(1970-)，男，硕士，副教授，主要研究方向：计算机软件，计算机网络，图书情报。

协调中心/联盟中心，D_0本身为一个安全自治域，主要负责资源/服务的组合与构建、资源访问权限和不同自治域属性信息之间的映射。$D_i(0<i<N+1)$为相对独立的安全自治域，每个自治域有各自的认证授权系统和资源服务。

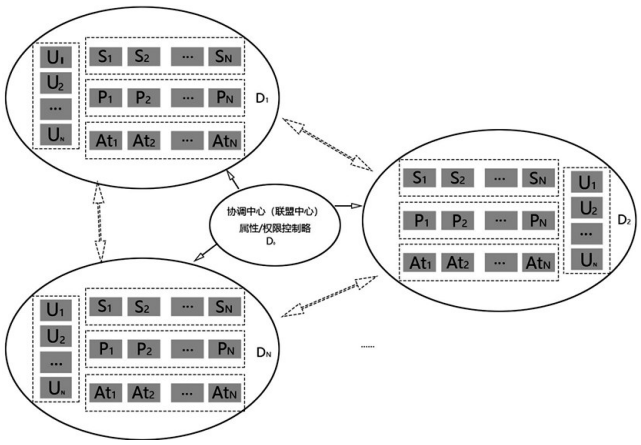

图1 系统总体架构

D_0在物理结构上可位于任一D_i中，但在逻辑上是一个独立的组织。

1.2 单域数据模型

用户得到授权后可以访问联盟组织内的共享资源。当用户访问联盟组织内本域的资源时，这是一个典型的单域访问控制架构，此时用户、服务和资源被同一个管理者所控制，其属性存取控制模型架构如图2所示。

从图2中可以看出单域存取控制模型是一个标准的(U,R,A,Op,Ob)五元组，其中U代表用户子集，R代表角色子集，A代表角色拥有的属性子集，Op代表操作集，Ob代表对象子集。

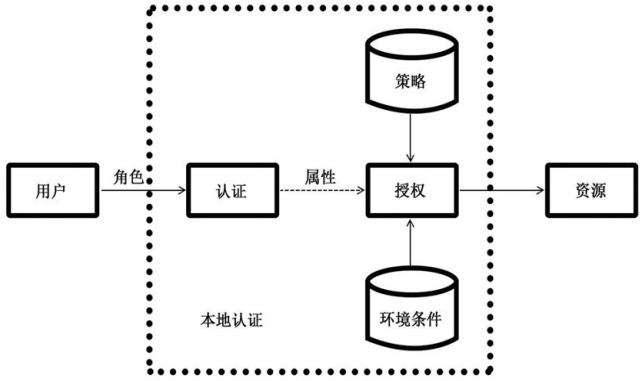

图2 基于属性存取控制的单域模型架构

设单域环境下基于属性/权限的分配策略为PR、权限集为Pe，则：

$Pe \subseteq 2^{(Op \times Ob)}$ 其中X为笛卡尔积操作。

PR=(U,A,Pe)

设属性集$A' \subseteq 2^A$，即$\{A' | A' \subseteq A\}$，自治域内属性/权限分配 $AP \subseteq A' \times Pe$，设a1,a2为A的两个元素，如果$(\{a1,a2\},P) \in AP$，则表示拥有属性集合{a1,a2}的实体拥有权限P。

1.3 多域数据模型

当用户通过联盟中心访问本联盟中外域的资源时，用户、属性、服务/资源和分配策略分别被不同的管理者所控制。用户首先进行本地认证，再通过协调中心的属性映射来实现跨域资源存取，其属性存取控制模型架构如图3所示。

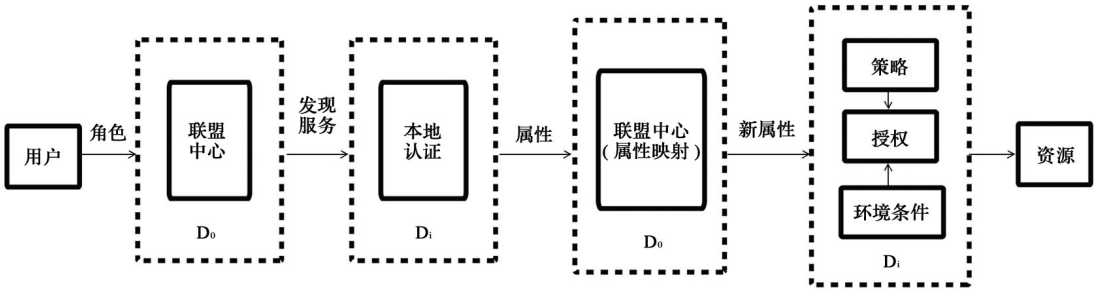

图3 基于属性存取的跨域访问模型架构

2 机制的实现

2.1 系统实现

2.1.1 问题分析与定义

参与跨域数据共享的所有自治域构成一个集合D，$D=\{D_0,D_1,D_2,...,D_N\}$，其中$D_0$代表协调中心。

设多域数据模型由N个自治域组成，$D_i(0<i<N+1)$为各个自治域，每个域的属性集记为A_i'，资源或服务的集合记为S_i'，整个基于联盟环境下的多域存取控制模型的属性集为A、资源或服务记为S，则：

$$A=1,\overset{\cup}{2},\cdots,N^{A_i'}$$

$$S=1,\overset{\cup}{2},\cdots,N^{S_i'}。$$

2.1.2 相关服务策略

对每个自治域而言，它们都是身份提供者IDP和资源提供者SP的统一体。

对每个IDP来说，它是一个(U，A，P)的三元组，U、A、P的定义同上，其中P=(U,A)，表示具有属性A的用户被赋予操作权限P；UA⊆(UXA)表示用户U具有属性A；AP⊆(AXP) 表示从属性到权限的映射。

对每个SP而言，它是一个(A，Op，Ob)的三元组，AS⊆(AXS) 表示从属性到服务的映射，在多域环境下，假设域集合用D_total表示、属性集合用A_total表示、操作对象集合用Ob'表示、权限集合用Pe'表示、整个联盟环境下访问控制机制的属性/权限集相关策略用AP'表示，Op各域一致，则有：

$D\_total=\overset{\cup}{i=1,2},\cdots,k^{D_i}$，(0<i<N+1)

$A\_total=\overset{\cup}{i=1,2},\cdots,k^{A_i}$，(0<i<N+1)；

$Ob'=\overset{\cup}{i=1,2},\cdots,k^{Ob_i}$；

$Pe'\subseteq 2^{(OP\ X\ Ob)}$。

$AP'\subseteq At''\ X\ Pe'$，其中$At''\subseteq 2^{At'}$，$At'\subseteq 2^{A\_total}$。

2.1.3 跨域属性映射

由于联盟环境下各个自治域之间的属性是相互透明的，本机制通过协调中心来建立各域属性之间的映射。

跨域属性映射的具体实现如下：

(Aa▷Ac)，Aa.d=Di,Ac.d=Dk，i≠k (1)[5]

上式表示将域Di中的属性Aa映射到域Dk中的属性Ac上

(Ab▷Ac)，Aa.d=Dj,Ac.d=Dk，j≠k (2)

上式表示将域Dj中的属性Ab映射到域Dk中的属性Ac上

跨域属性映射，是构建基于属性/权限相关服务上的一个映射，从(1)和(2)两式得出：

(Aa▷Ab)，Aa.d=Di,Ab.d=Dj，i≠j

将域Di中的属性Aa映射到域Dj中的属性Ab上，从而使域Di中的属性Aa和域Dj中的属性Ab具有相同的属性值时具有相同的权限。

2.2 工作流

通过前面的定义和分析，结合系统的实现，一个正常的跨域授权服务工作流程如图4所示主要包含以下几个步骤。

(1) 用户向目标域中的资源发出访问申请。

(2) 系统通过发现服务将用户重新定向到用户所在安全域进行认证[6]。

(3) 通过认证的用户，将一个含有本地属性的令牌发送到协调中心。

(4) 协调中心通过属性映射，将包含有新属性的外地令牌传送到目标域。

(5) 目标域结合本地策略和环境条件对属性进行验证。

(6) 如果通过验证，则允许用户访问资源。

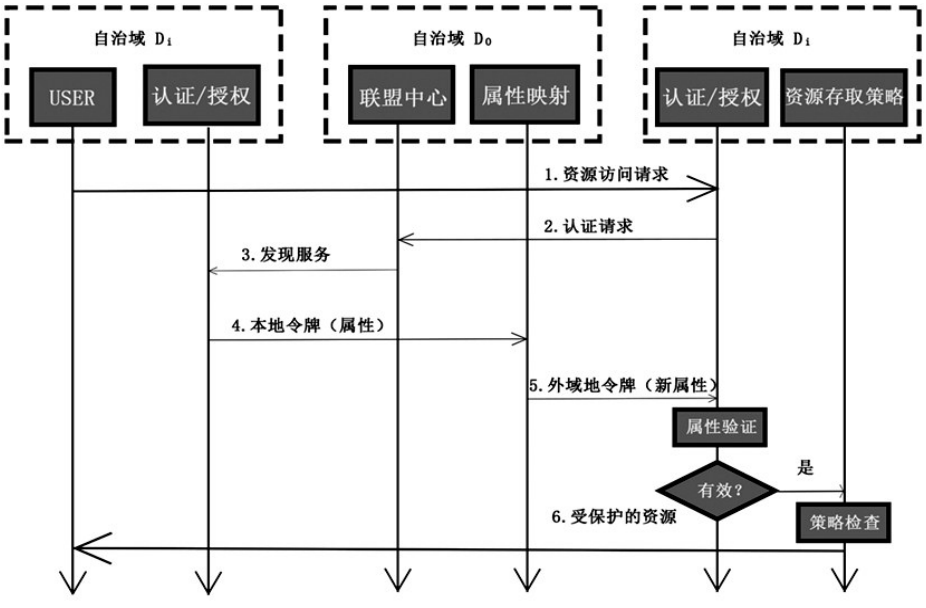

图4 跨域授权服务工作流程图

(下转第20页)

成,解决了智慧农业系统中不同应用需求的数据交换与共享,为物联网在农业领域的应用及系统的设计实现提供了一定的参考,但还需要进一步的完善,尤其是如何对获取的数据进一步的过滤及深度数据挖掘和分析、对服务的详细定义、调用接口的定义及性能描述等仍需要进一步的研究。

参考文献(References):

[1] Biggs P,Srivastava L.ITU Internet reports 2005: the internet of things[M].Geverna: International Telecommunication Union,2005.

[2] 李道亮.农业物联网导论[M].科学出版社,2012.

[3] 葛文杰,赵春江.农业物联网研究与应用现状及发展对策研究[J].农业机械学报,2014.45(7):222-230

[4] PRESSER M, BARNAGHI P M, EURICH M. The sensei project: Integrating the physical world with the digital world of the network of the future. Ieee Communications Magazine,2009.47(4):1-4

[5] JOACHIM W W. Initial architectural reference model for IoT. EU FD 7 Project, Deliverable Report: D1.2,2011.

[6] 姜洋,王雷.基于SOA思想的农产品质量追溯系统框架[J].湖北农业科学,2012.51(19):4369-4373

[7] GUBBI J, BUYYA R, MARUSIC S, PALANISWAMI M. Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 2013.29(7):1645-1660

[8] 杨斌,张卫冬,张利欣,章立军,时鹏.基于SOA的物联网应用基础框架[J].计算机工程,2010.36(17):95-97

[9] 沈苏彬,范曲立,宗平,毛燕琴,黄维.物联网的体系结构与相关技术研究.南京邮电大学学报(自然科学版), 2009.29(6):1-11

[10] 高洁天,朱森林,常歌,符凌峰,黄震宇.基于农业物联网的智能温室系统架构与实现[J].农机化研究,2018.1:183-188

[11] 郑纪业,阮怀军等.农业物联网体系结构与应用领域研究进展[J].中国农业科学,2017.50(4):657-668

[12] 凌晓东.SOA综述[J].计算机应用与软件,2007.24(10):122-124

[13] 朱振杰.SOA的关键技术的研究与应用实现[D].电子科技大学,2006.

[14] 傅兵.基于SOA的数字农务系统关键技术研究[D].南京农业大学,2012.

[15] 叶钰,应时,李伟斋,张韬,面向服务台体系结构及其系统构建研究[J].计算机应用研究,2005.

[16] 唐珂.国外农业物联网技术发展及对我国的启示[J].农业物联网,2013.28(6):700-707

[17] 刘颖.物联网环境下超高频射频识别系统中多卡识别的实现[J].微电子学与计算机,2017.34(11):104-107

[18] 杨玉霞,汤金金.太阳能农机发动机监测系统设计[J].农机化研究,2018.5:259-263

[19] 梅宏.软件中间件技术现状及发展[M].清华大学出版社,2004.

[20] 程宏杰,朱震宇,陈泽.农业物联云的设计与实现[J].江苏农业科学,2017.45(3):179-183

(上接第16页)

3 结束语

本文研究了联盟环境下多自治域之间资源访问控制问题,考虑到各个安全域的独立性和用户隐私等特点,在单域RBAC访问控制的基础上,构建了基于属性的跨域认证授权机制。基于属性的存取控制和协调中心的权限策略的通用认证和授权架构支持不同的认证技术,保留并利用了各个自治域原有的认证系统;每个自治域保持资源联盟的独立性,在此基础上实现身份透明的属性聚合方案,并且保护了用户隐私。本机制可满足大型企业和联盟组织之间的资源共享,在实际应用中有较大的价值,该机制在Windows平台下已经实现并得以应用,Linux平台下的设计和实现将是下一步努力和研究的方向。

参考文献(References):

[1] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-Based access control models. IEEE Computer, 1996.29(2):38-47

[2] Ferraiolo D, Sandhu R.Proposed NIST Standard for Rolebased Access Control[J]. ACM Transactions on Information and System Security,2001.4(3):224-274

[3] 申巍葳,王宝生,贺建忠.一种面向公共服务的跨域授权模型的研究及实现[J].国防科技大学学报,2011.10:123-127

[4] Vincent C. Hu,David Ferraiolo,Rick Kuhn,Adam Schnitzer, Kenneth Sandlin,Robert Miller,Karen Scarfone,Guide to Attribute Based Access Control(ABAC) Definition and Considerations.http://dx.doi.org/10.6028/NIST.SP.800-162

[5] 张帅,孙建伶,徐斌,黄超.KAVSAleksanderJ,基于RBAC的跨多企业服务组合访问控制模型[J].浙江大学学报,2012.11:2037

[6] 刘其群,跨域认证授权机制的研究[J].河南农业,2017.8:58-59