**基于多元属性访问控制机制**

**引言**

在大数据和云计算环境中，安全有效的访问控制机制是保障数据服务共享信息平台安全的重要技术措施。访问控制实际上就是根据实际需求和安全性考虑，制定访问规则或策略，用来控制用户对数据或服务的访问。

当前信息环境中的数据服务具有多样性、动态性、匿名性和异构性等特点，细粒度的访问控制变得十分困难，面临着诸如用户和资源海量多样，访问环境动态变化，信息环境具有多域特征，访问需求细粒度等困难。传统的访问控制机制很难适应当前需求，基于属性访问控制成为研究热点，得到广泛发展和应用。

本文针对基于属性访问控制机制的特点和不足之处，结合多元属性和控制策略自身特点，采用策略树和LSSS属性矩阵的思想设计算法，从而实现高效、安全、细粒度的访问控制。

**1、相关研究**

访问控制一直都是信息安全研究的重点问题，不论是传统的IT、互联网领域，还是物联网领域，访问控制在其中都扮演着重要的角色，对于保证服务器软硬件、资源和用户数据的安全性起着举足轻重的作用。

传统的访问控制机制已经无法适应当前大数据和云环境下的数据服务访问，自主访问控制（DAC）[1]在用户和资源非常庞大时，分散的访问权限变得难以管理，效率低下；强制访问控制（MAC）[2]过于严苛，灵活性差，实现困难；基于角色访问控制（RBAC）[3]在开放式的环境中效率不高，授权不够灵活。因而都很难适应当前环境。

基于属性访问控制(Attribute-Based Access Control ABAC)思想源于信任管理及其扩展[4-6]，文献[7]和文献[8]分别提出基于主客体属性的访问控制矩阵模型ABAM和用有限集合论描述主、客体属性的访问控制逻辑框架LABAC，二者对属性描述均为粗粒度，也没有给出访问控制具体实现方法。ABAC模型考虑用户、资源、操作、执行动态请求时的运行上下文与授权相关的各种属性，细化了访问控制的粒度，ABAC模型及其扩展模型[9-11]能够根据用户、资源、动作和运行上下文的属性动态的进行授权，具有更好的灵活性和扩展性。

属性基加密机制[12]是利用属性值对数据机密性进行保障的密码机制，自Sahai和Waters提出该类方案[13]以来，得到广泛研究和应用，尤其是云计算、云环境兴起后，属性集加密机制发展迅速。其核心是如何将秘密拆分并映射到不同的访问控制属性集上。

基于LSSS（Linear-Secret-Sharing Schemes）的共享矩阵是一种将访问策略和属性集相结合转化到一个关联矩阵的方案，通过矩阵的运算减少大量子秘密和属性集进行匹配运算过程的开销，得到广泛应用。文献[14]提出的算法可对“（n，t）门限策略”的各参与方进行处理，构造规范化的共享矩阵。文献[15]提出对“AND/OR策略”进行

1. **准备知识**

**2.1、多元属性划分**

不同于传统的访问控制模型（DAC，MAC以及RBAC等），基于属性的访问控制（ABAC）是由参与访问请求的主客体及当前访问环境等多方面的属性来决定的，属性在这里是指访问控制过程中用来描述用户、数据资源、访问环境和操作请求等性质的特征。结合当前研究成果和实际需求，可对属性进行如下划分和定义：

**定义2.1**：访问控制结构，由四元组（S，O，E，Act）组成，其中，S={}代表主体属性集合，O={}代表客体属性集，E={}代表环境属性集，Act={}代表操作属性集，上述集合中n1。

**定义2.2：**主体属性集，对于任意∈S，i=1,2,3…n，则有描述当前访问请求访问主体的属性集。

**定义2.3：**客体属性集，对于任意∈O，i=1,2,3…n，则有描述当前访问请求被访问客体的属性集。

**定义2.4：**环境属性集，对于任意∈E，i=1,2,3…n，则有描述当前访问请求访问环境的属性集。

**定义2.5：**操作属性集，对于任意∈Act，i=1,2,3…n，则有描述当前访问请求访问操作的属性集。

本文的访问控制机制都是基于上述四类属性集合所构成的四元组，综合多种属性进行访问权限计算和验证。

**2.2、策略表达式**

访问控制策略是访问控制的基础和核心，对于访问控制功能模块，合理安全的访问控制策略是不可或缺的内容。访问控制策略则是由一个或多个属性通过逻辑关系组合而成，组成策略的各个属性可构成策略属性集。多个策略属性集内的所有属性共同构成策略属性域。

**定义2.6：**策略属性集，对于策略内所包含的任意一个属性，j=1,2,3…，都有∈，且，则={,,…}表示策略的策略属性集。

**定义2.7：**策略属性域Z，对于任意策略内的任意属性，都有∈Z，则Z={}表示所有策略属性集内包含的属性共同构成的策略属性域。

为了实现动态、安全、细粒度的访问控制，本文对访问控制策略进行规范化的描述，主要分为门限策略表达式和与或策略表达式两类。

门限策略主要针对策略属性集内包含多个属性的策略，采用（n,t）门限条件的方式构成，其中n为策略属性集内属性的个数，t为策略的门限条件。

与或策略主要是针对两个单一的属性，采用逻辑与（∧）、逻辑或（∨）两种逻辑运算符连接而成。

实际上，与或策略又可以看作是门限策略的特例，即（2，t）门限条件，t=1表示或策略，t=2表示与策略。因而本文采用一种的规范化表达式对上述两种类型的策略进行整理，从而保证策略的完备性和一致性。

**定义2.8：**

**（1）**访问控制策略P=(,t),为组成访问控制策略的子策略，当子策略的个数大于等于t时，满足访问控制策略的约束条件。否则，不满足控制策略的约束条件。

**（1）**访问控制策略=(,t),为组成访问控制策略的属性，当属性的个数大于等于t时，满足访问控制策略的约束条件。否则，不满足控制策略的约束条件。

1. **基于多元属性访问控制机制设计**

**3.1**

**3.2**

1. **实验结果**

**4.1实验环境**

本次实验是在Win10系统上，通过JAVA开发得以实现。实验相关数据通过在本机模拟得到，软硬件的环境如表1所示。

表1 实验环境

|  |  |  |
| --- | --- | --- |
| 硬件环境 | CPU | Intel(R) Core(TM) i5-2450M 2.50GHz |
| Memory(RAM) | 4.00GB |
| Disk | 500GB |
| 软件环境 | OS | Windows10 64-Bit |
| 开发工具 | Java Version | Java 1.7.0\_80 |
| Compiler | Intellij IDEA 15.0.2 |
| Database | MySQL 5.7 |

**4.2实验验证**

实验分别从功能验证和效率验证两方面进行验证，得到如下结果。

**4.2.1功能验证**

实验分别对预先设置的5条访问控制策略进行处理和描述，表示访问控制策略内的任意属性，。

访问策略描述如表2：

表2 访问控制策略

|  |  |  |
| --- | --- | --- |
| 编号 | 访问控制策略 | 策略属性集 |
| 1 |  | {} |
| 2 | 与 | {，} |
| 3 | 或 | {，} |
| 4 | (,)中至少有2个 | ,} |
| 5 | {;,)中至少有两个;或}全部满足 | ,,} |

对发送访问请求的多个用户进行权限验证，实验结果如表3:

表3 实验结果

|  |  |  |
| --- | --- | --- |
| **访问控制策略** | **基于属性访问控制机制** | **验证结果准确率** |
| 1 | （, 1） | 100% |
| 2 | （,,1） | 100% |
| 3 | （,,2） | 100% |
| 4 | （,,,2） | 100% |
| 5 | （,,,2),(,,1),3） | 100% |

**4.2.2效率验证**

实验选取，属性域的大小为100。随机生成五组访问控制策略，每组策略的属性集大小分别为1，2，5，10。设置三组用户，用户的数目分别为1，100，10000.依次采用门限策略机制、与或策略机制和基于属性访问控制机制对三组用户进行权限验证，时间开销设为T1，T2，T3。实验结果如表4:

表3 实验结果

|  |  |  |  |
| --- | --- | --- | --- |
| 用户数量  属性集大小 | 1 | 100 | 10000 |
| 1 | T1=T2=T3 | T1=T2=T3 | T1=T3>T2 |
| 2 | T1=T2=T3 | T1>T2=T3 | T1>T3>T2 |
| 5 | T1=T2=T3 | T2>T1=T3 | T2>T1>T3 |
| 10 | T2>T1 =T3 | T2>T1=T3 | T2>T1>T3 |

实验结果可以看出，随着属性集大小的增长，与或策略机制的效率逐渐降低；随着用户数目的增多，门限策略机制的效率逐渐降低。因而针对大数据和云计算环境下海量的用户和属性，本文提出的基于属性访问控制机制可以有效地实现对于用户权限的验证和控制，在时间开销上又比单一的门限策略机制和与或策略机制小。

参考文献:

[1]Conway R W,Maxwell W L,Morganhl.On the implementation of security measures information systems[J].Communications of the ACM,1972,15(4):211-220.

[2]Denning D E.A lattice model of secure information flow[J].Communications of the ACM,1976,19(5):236-243.

[3]Bharadwaj V,Baras J.Towards Automated Negotiation of Access Control Policies[C].In:Proceedings of IEEE International Workshop on Policies for Distributed Systems and Networks.Los Alamitos,USA:IEEE Computer Society Press,2003:111-119.

[4]Bhatti R,Bertino E,Ghafoor A.A Trust-Based Context-Aware Access Control Model for Web-Services[C].Proceedings of IEEE International Conference on Web Services.San Diego,USA:IEEE Press,2004:184-191.

[5]Blaze M,Feigenbaum J,Lacy J.Decentralized trust management[C].Proceedings of the 17th Symposium on Research in Security and Privacy.Oakland,CAlIEEE computer Society Press 1996:164-173.

[6]Weeks S.Understanding trust management systems[C].Proceedings of the 2001 IEEE Symposium.on Security and Pricacy.Washington,USA:IEEE Computer Society Press,2001:94-105.

[7]Zhang X,Li Y,Nalla D.An attribute-based access matrix model[C].Proceedings of the 2005 ACM Symposium on Applied Computing.Santa Fe,New Mexico:ACM Press,2005:359-363.

[8]Wang L Y,Wijesekera D,Jajodia S.A logic-based framework for attrubute bassed access control[C].Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering.New York,USA:ACM Press,2004:45-55.

[9]B Lang,I Foster,F Siebenlist,et al.A flexible attribute based access control method for grid computing[J].Journal of Grid Computing,2009,7(2):169-180.

[10]R Bobba,O Fatemieh,F Khan,et al.Using attribute-based access control to enable attribute-based messaging[C].Proceedings of the 22nd Annual Computer Security Applications Conference on Annual Computer Security Applications Conference.Washington,USA:IEEE Computer Society,2006:403-413.

[11]C Ye,Z Wu,Y Fu.An attribute-based delegation model and its extension[J].Journal of Research and Practice in Information Technology.2006,38(1):3-17.

[12]苏金树,曹丹,王小峰等.属性基加密机制.[J].软件学报.2011,22( 6) : 1299-1315．

[13]Sahai A,Waters B.Fuzzy identity-based encryption.[A].Aarhus:Advances in Cryptology-EUROCRYPT 2005［C］.Berlin:Springer,2005.457-473．

[14]Liu Z,Cao Z. On Efficiently Transferring the Linear Secret-Sharing Scheme Matrix in Ciphertext-policy Attribute-based Encryption[EB/OL].http://eprint.icar.org/2010/374.pdf,2010-07-06/2014-02-26.

[15] Sushmita R,Amiya N,Ivan S. DACC: Distributed Access Control in Clouds.[C].Trust Security and Privacy in Computer and Communications(TrustCom),2011 IEEE 10th International Conference on 2011:91-98.