普适计算环境下的安全分布式访问控制系统研究

窦文阳 王小明 张立臣
(陕西师范大学计算机科学学院 西安 710062)

摘 要 针对普适计算环境下复杂的安全需求,设计了一个安全分布式访问控制系统。在系统体系结构设计中,提出了一个分布式授权查询算法,解决了普适访问控制系统授权查询的效率问题;引入授权模糊推理器,实现了普适访问控制的模糊推理授权。最后给出了一种加密机制,从而保证了系统在授权查询过程中信息的保密性和完整性。

关键词 普适计算,模糊访问控制,区间值模糊推理,分布式授权
中图法分类号 TP309 **文献标识码** A

Research on Secure Distributed Access Control System for Ubiquitous Computing

DOU Wen-yang WANG Xiao-ming ZHANG Li-chen
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract This paper designed a secure distributed access control system for complex security requirements in ubiquitous computing environment and the system architecture was presented. A authorization query algorithm was proposed to solve the problem of the efficiency of authorization query. Fuzzy reasoning machine was proposed to achieve fuzzy authorization. Finally, an encryption mechanism was presented to ensure the confidentiality and integrity of information during the process of authorization query.

Keywords Ubiquitous computing, Fuzzy access control, Interval-valued fuzzy reasoning, Distributed authorization

1 引言

普适计算(Ubiquitous/Pervasive Computing)是继主机计算、桌面计算之后发展起来的一种新的计算模式。普适计算思想最早是1991年由Mark Weiser提出的,其目标是建立一个充满计算和通信能力的环境,同时使这个环境与人们逐渐地融合在一起[1]。在这个环境中,使用计算设备就像使用水、电等生活必需品一样方便,人们注意的中心将回归到要完成的任务本身。目前,普适计算已经被国内外学术界和工业界公认是未来计算的主流模式,它将对计算机应用产生深刻的影响[2]。

长期以来,普适计算研究工作主要集中在其基础设施上,例如智能空间管理技术、新设备及其连接技术、普适计算的软件中间件技术等[3]。但是,随着研究和应用的不断深入,普适计算的安全性越来越重要,并已成为普适计算研究的一个基础问题[4]。访问控制依据预先定义的授权策略授予主体访问客体的权限,并对主体使用权限的过程依据预先定义的访问控制策略进行有效控制,从而实现系统资源的有权访问,防止非授权的信息泄露,它是确保计算系统安全的核心技术之一。访问控制由于对复杂计算系统的安全控制十分有效,因此是实现普适计算安全的关键技术[5]。然而,现有的访问控制系统主要是基于中心服务器的封闭式静态授权系统,没有考虑授权所处的环境对访问控制的影响,所以不能完全适用于开放式、动态的普适计算环境[6]。

普适计算环境下的访问控制系统面临以下安全挑战:

(1)设备分散无中心的拓扑结构要求访问控制系统不能是基于中心服务器的集中式结构;

(2)普适设备能量、计算能力、存储空间及带宽的相对有限决定了访问控制系统授权算法必须简单、高效;

(3)普适计算环境的复杂性要求访问控制系统支持多种安全策略,同时允许用户设定自己的访问控制规则;

(4)普适计算环境下的安全问题具有模糊性,要求普适访问控制能够描述具有模糊性的安全控制策略,同时支持对不完备上下文信息进行模糊推理授权。

针对以上问题,本文的主要工作如下:

(1)设计了一个普适计算环境的安全分布式访问控制系统体系结构,通过引入模糊推理器,实现了对不完备上下文信息的模糊推理授权和系统安全强度的自适应控制,为智能化访问控制系统设计提供了新思路;

(2)提出了由资源服务器、授权服务器和授权原子谓词服务器构成的分布式授权查询模块,解决了普适计算环境下高效授权查询问题,并给出了相关实现算法;

(3)提出了一个加密机制,保证了分布式授权信息查询过程中信息的保密性和完整性。

本文第2节为相关研究;第3节提出了一个安全分布式访问控制系统体系结构,对分布式授权查询和模糊推理器的

到稿日期:2012-08-13 返修日期:2012-11-14 本文受国家自然科学基金项目(60970054,61173094)资助。
窦文阳(1979-),男,博士,主要研究方向为网络与信息系统安全、访问控制等,E-mail:douwenyang@snnu.edu.cn;王小明(1964-),男,博士生导师,主要研究方向为网络与信息系统安全、工作流系统安全等;张立臣(1979-),男,博士,主要研究方向为信息系统安全等。

设计进行了详细介绍；第 4 节给出了一种授权查询信息加密机制；最后总结全文。

2 相关研究

目前普适计算环境下的访问控制研究主要思路是基于传统的访问控制技术进行适应性扩展，但是由于普适计算环境复杂性和多样性的特点，扩展的访问控制系统在实际使用中都存在一些不足。例如，文献[7]扩展了 RBAC 模型，给出了一个普适计算环境下的上下文感知的动态访问控制模型，但是上下文信息动态变化造成了角色的复杂性，普适设备能源的有限性无法处理这种复杂关系，阻碍了模型的实际应用；文献[8]在使用控制模型基础上，提出了一个普适访问控制模型，该模型支持多安全策略和动态授权，但其不足是集中式授权方式不适用于结构分散的普适计算环境。关于普适访问控制的另一种研究思路是基于信任模型进行扩展，通过信任管理来实现资源的安全分布式控制。例如，文献[9-11]对普适计算环境下的动态信任模型进行了研究，作者根据信任策略为实体制定不同的信任关系，依据实体间的信任关系确定实体的访问权限。但是在普适计算环境中，用户和设备的多样性及动态性，以及虚拟匿名的潜在合作使得这种信任关系在实际应用中难以建立。

在普适访问控制系统的研究中，文献[12,13]分别给出了基于用户位置和环境上下文的访问控制系统体系结构，系统支持动态授权，并且加强了对用户安全隐私信息的保护，但不足的是都不支持多种安全策略；文献[14]给出了一个基于 Web Service 的普适访问控制系统的体系结构 Open Ambient。在 OpenAmbient 中根据上下文信息动态决定授权结果，但是系统设计中没有解决上下文信息的高效查询问题，使得集中式结构成为系统运行的瓶颈。文献[15]给出了一个上下文感知的动态访问控制体系结构，但没有解决普适计算环境下安全控制的模糊授权问题。

普适计算环境下的安全问题具有高度的模糊性和不确定性[7]。支持对模糊性安全控制策略的描述，以及对授权过程中不完备上下文信息的推理决策直接决定着普适访问控制系统授权结果的正确性。现有的工作中对这方面的研究还较少。文献[16-18]对普适计算环境下的访问控制模型进行了研究，解决了普适环境下的模糊授权问题，但是缺少从系统实现方面的进一步研究。

3 普适访问控制系统

本节提出了一个普适计算环境下的安全分布式访问控制系统体系结构，对分布式授权系统和模糊推理器的设计进行了详细介绍，给出了相关实现算法。

3.1 系统体系结构

在基于规则的访问控制模型中，访问控制策略可以通过一条或多条授权规则进行描述，因此基于规则的访问控制模型具有支持多安全策略的特点。本文在基于规则的访问控制模型的基础上，设计了一个普适计算环境下的安全分布式访问控制系统(Secure Distributed Access Control for Ubiquitous Computing，简称 SDAC)，该系统支持多安全策略的分布式、动态模糊授权。

图 1 给出了 SDAC 系统的体系结构。SDAC 没有使用唯一的中心授权服务器进行授权决策，而是通过资源服务器 RS (Resource Server)、授权服务器 AS(Authorization Server)、授权原子谓词服务器 APS(Atom Predication Server)组成的分布式系统进行授权推理决策。当系统收到用户的授权请求时，首先将授权请求转化为相应的授权查询，然后依据授权规则将授权查询分解为多个子查询任务，再把这些子查询任务发送给不同的授权原子谓词服务器进行验证，最终的授权结果是对子查询任务的综合决策。为了实现普适环境下对不完备上下信息的模糊授权，本文提出了一种模糊访问控制规则，SDAC 通过模糊推理器进行模糊推理授权。

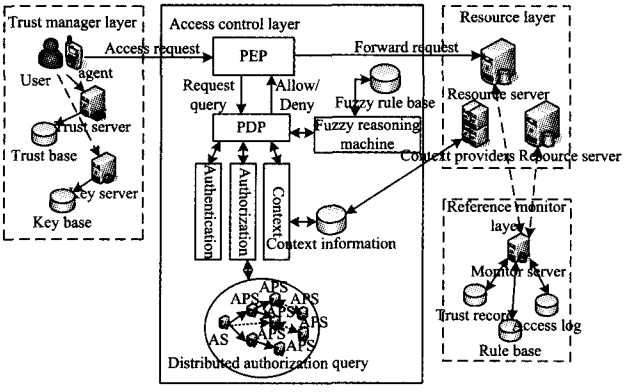

图 1 SDAC 系统体系结构

SDAC 主要由信任管理层(Trust Manager Layer)、访问控制层(Access Control Layer)、监视层(Reference Monitor Layer)和资源层(Resource Layer) 4 部分组成，各部分功能说明如下：

(1)信任管理层。信任管理层主要是管理用户和设备的信任关系。当一个用户或设备进入环境时，需要登录信任管理服务器(Trust Server)获取信任值，再进行授权访问。如果是匿名用户或未知设备，则要为其分配相应的初始信任值。此外，在信任管理层还为每个用户及设备分配一对公钥/私钥(Public key/ Private key)，以保证在无线网络环境下信息通讯的保密性(本文第 4 节将对授权查询过程中信息加密机制进行详细说明)。

(2)访问控制层：访问控制层是系统授权决策的核心部分，主要由 7 个模块构成，分别是：

①策略执行模块(Policy Enforcement Point，PEP)，主要功能是接收用户的访问请求，然后转发到策略决策模块(PDP)，根据 PDP 返回结果，决定对用户授权请求 Allow/Deny；

②策略决策模块(Policy Decision Point，PDP)，主要功能是根据 PEP 发送的用户访问请求建立授权查询，通过认证模块、授权模块、上下文模块及模糊推理器综合得出授权决策结果，再把结果返回给 PDP；

③认证模块(Authentication)，主要完成用户的认证工作，在普适计算环境下应该支持多种认证方式，不同的认证方式相应的信任程度也是不同的，认证模块也为信任管理层提供与信任评价相关的认证信息；

④授权模块(Authorization)，完成对 PEP 发送的授权请求的验证，传统的授权查询是基于中心服务器完成的，本文设计了一个分布式的授权查询系统，分布式授权查询通过分布式授权查询模块完成；

⑤上下文模块(Context)，与资源层上下文服务器(Con-

text Providers)共同完成对环境上下文信息及事实的收集工作，上下文信息包括了系统上下文、用户上下文、资源上下文等；

⑥模糊推理器(Fuzzy Reasoning Machine，FRM)，与 PEP 共同完成模糊授权推理(本文第 3.3 节将对 FRM 授权推理过程进行详细说明)；

⑦分布式授权查询模块(Distributed Authorization Query)，由一组 AS 和 APS 构成，完成分布式授权查询工作(第 3.2 节给出相关实现算法)；

⑧模糊规则库(Fuzzy Rule Base)，通过模糊规则来描述普适环境下的复杂、模糊性安全控制策略，实现对资源和权限的有效控制(本文第 3.3 节给出了一种模糊访问控制规则的定义和推理过程)。

在 SDAC 系统中我们主要定义了 3 种类型规则：a)模糊授权规则，用于完成对用户授权请求的推理决策，例如可以定义模糊授权规则：如果用户在智能会议室内的可能性较高，则授予用户对打印机使用权限的强度较高。b)模糊访问控制规则，用于对资源使用权限的动态控制，例如可以定义模糊访问控制规则：如果用户授权强度在[0.6，0.8]之内，则授予用户所请求的访问权限。系统中资源安全强度可以随上下文环境变化，当资源安全强度变化，用户权限使用的状态也将随之动态改变，以实现动态访问控制授权管理。c)系统安全强度控制规则，SDAC 的安全强度是变化的，这种变化是通过定义安全强度控制规则进行调节控制的。当环境的上下文条件发生变化时，系统对资源的安全控制强度也将随之变化。对安全强度的控制是通过安全强度控制规则来调节的。

(3)监视层。监视层是系统访问控制的具体实现。它的主要工作是监视系统权限的使用状态，如果有相关事实或上下文信息发生变化，需要重新对系统内的授权进行判断。特别需要对用户权限的使用状态进行监控，如果用户的上下文信息与系统的授权规则冲突，则立即终止用户正在使用的权限。监视层可以使用主动数据库触发技术来实现。

(4)资源层。资源层主要管理环境中的资源和设备，具体工作由资源服务器(RS)完成。资源服务器管理本地环境资源，提供共享资源的设备也可以成为其资源的管理服务器。资源层还通过上下文服务器(Context Providers)为授权层提供上下文信息，用于授权决策。

3.2 分布式授权查询

分布式授权查询是 SDAC 的核心部分。下面首先通过一个实例来说明授权分解和分布式授权过程。

例 1　如图 2 所示，图中 RS 是资源服务器；AS_1－AS_4 是授权服务器，APS_1－APS_4 是授权原子谓词服务器。图中实线箭头表示授权查询的发送，虚线箭头表示查询结果的返回。每个 AS 都有本地规则库(Rule Base)，用于对授权请求进行分解。为了便于说明，图中使用 $C \leftarrow A \wedge B$ 的形式表示授权规则，其含义为：如果 A 和 B 同时满足，则 C 成立。

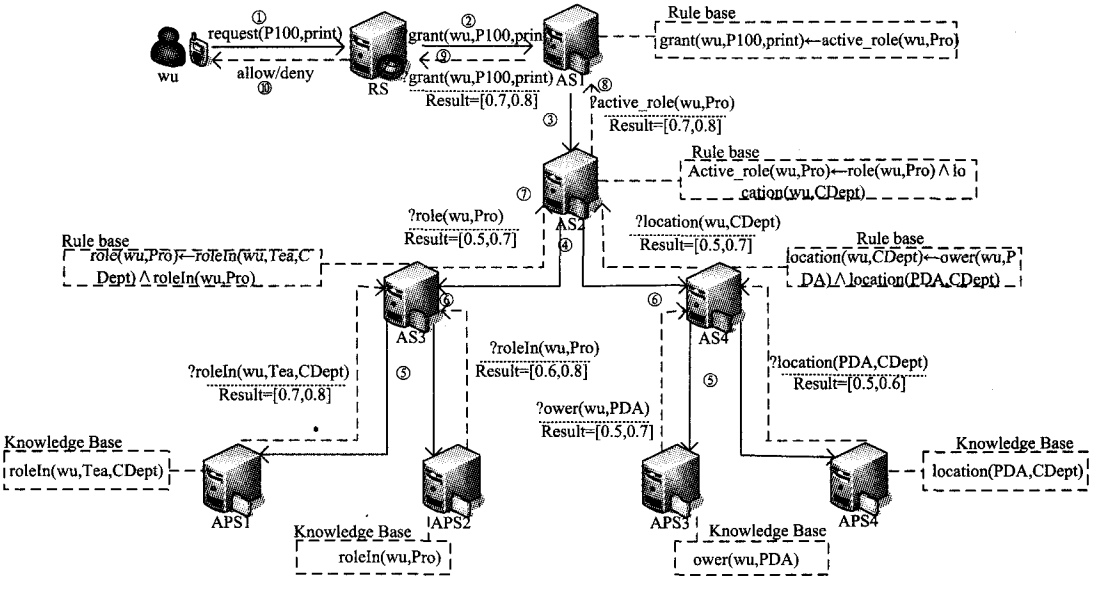

图 2　分布式授权查询示意图

在图 2 中，用户 wu 提出了对打印机 P100 打印权限 print 的授权请求，授权过程如下：

(1)wu 提出授权请求 request(P100，print)，并发送给管理 P100 的 RS。

(2)RS 收到 request，建立授权请求 q_1 =?grant(wu，P100，print)，再把 q_1 发送给 AS_1 进行授权查询。

(3)AS_1 收到 q_1，基于本地 Rule Base 对 q_1 进行分解，q_1 成立需要满足条件 active_role(wu，Pro)。由于 AS_1 不能对 active_role (wu，Pro)继续进行分解，因此只能建立子查询 q_2 =?active_role (wu，Pro)，再把 q_2 发送给所信任的 AS_2 进行查询。

(4)AS_2 接收 q_2，根据本地 RuleBase 进行分解，active_role (wu，Pro)成立需要满足两个条件：role(wu，Pro)和 location(wu，CDpet)。之后，AS_2 对自己不能完成分解的查询 role(wu，Pro)和 location(wu，CDpet)建立子查询 q_3 =?role (wu，Pro)和 q_4 =?location(wu，CDpet)，再把 q_3，q_4 分别发送给 AS_3，AS_4 继续进行查询。

(5)AS_3 接收到 q_3 对其进行分解，得知 q_3 成立需要满足 roleIn(wu，Tea，CDept)和 roleIn(wu，Pro)两个条件，然后建立两个子查询 q_5 =?roleIn(wu，Tea，CDept)和 q_6 =?roleIn (wu，Pro)，再分别发送到 APS_1，APS_2 进行验证。类似地，AS_4 对 q_4 进行分解，建立子查询 q_7 =?ower(wu，PDA)和 q_8 =?location(PDA，CDpet)，再分别发送到 APS_3，APS_4 进行验证。

(6)APS_1 接收 q_5，根据本地 Rule Base 进行验证，用户 wu 对 q_5 的满足程度在 0.7 到 0.8 之间，然后把查询结果返回给 AS_3。类似地，APS_2 把 q_6 的查询结果返回给 AS_3；同时，APS_3 接收 q_7，并根据本地 Rule Base 进行验证，得知用户 wu 对 q_7 的满足程度在 0.5 到 0.7 之间，然后把查询结果返回给 AS_4。类似地，APS_4 把 q_8 的查询结果返回给 AS_4。

(7)AS_3 收到 APS_1、APS_2 返回的 q_5、q_6 查询结果后，根据本地规则库对 q_5、q_6 进行模糊综合，再把综合后的结果返回给 AS_2。类似地，AS_4 对 APS_3、APS_4 返回的查询结果 q_7、q_8 进行模糊综合，再返回给 AS_2。

(8)AS_2 接收到 AS_3、AS_4 返回的结果后，根据本地的授权规则进行模糊推理，把得到的结果返回给 AS_1。

(9)AS_1 根据 AS_2 的结果，通过本地授权规则推理得到 q_1 的结果，并返回给 RS。

(10)RS 根据 AS_1 的授权查询结果，结合本地的安全阈值，做出最终的授权决策 Allow 或 Deny，然后返回给用户 wu，完成授权过程。

在例 1 中，AS 收到授权查询后，根据本地 Rule Base 对授权查询进行分解，得到多个子查询，然后把这些子查询发送到 APS 进行验证。APS 根据本地 Rule Base 对子查询进行验证，把验证结果(是一个区间值，表示满足的程度)返回给 AS。如果某一个 AS 不能完成授权查询工作，它将把不能完成的工作发送给其他信任的 AS，继续完成授权查询。最后，每个得到的子查询验证结果也不再是真值或假值，而是一个表示授权满足程度的区间值。系统将对多个子查询结果进行综合，再根据系统的安全阈值决定用户最终的授权结果。所以，整个系统授权工作不依赖于任何中心设备分布式进行，也不会因为某个服务器的停机而受到影响。AS 负责对授权请求进行分解以及对结果进行模糊综合，实际的查询验证工作由不同的 APS 完成，所以 AS 也不会成为系统的瓶颈。另外，通过这种授权分解模式，还可以有效增强系统的安全性。因为不同的 AS 只是处理部分授权查询工作，所以即使某个 AS 被入侵，入侵者也只获取部分查询的信息，不会泄露所有信息。例如在图 2 中，AS_3 如果只能知道 APS_1 和 APS_2 返回的查询结果，则并不能得到 APS_3、APS_4 的查询结果。同样地，AS_2 只有 AS_3、AS_4 的结果，并不能获得 APS_1、APS_2、APS_3、APS_4 返回的查询结果。所以，即使 AS_3、AS_2 被入侵，入侵者也只能获取部分信息，保证了信息的安全性。

下面给出授权分解实现的相关算法。算法 AUTH 是授权算法，授权过程是：先将用户的授权请求 Re 转化为授权查询 Q，然后基于本地规则库对 Q 进行分解，如果本地规则库没有相关规则可以分解 Q，则将 Q 发送到其他 APS 进行分解。最后将授权查询分解为多个子条件 $c_1, c_2, \cdots, c_n$，然后系统将多个子条件的实际满足程度 $c_1', c_2', \cdots, c_n'$ 通过模糊推理器 FRM 进行模糊综合，如果结果大于系统预先定义的授权阈值 μ，则授予权限；否则，拒绝授权。DEQU 算法是授权查询分解算法，通过递归将查询分解为多个子条件，再由系统分别去查询各个子条件的满足程度。

Algorithms: AUTH

Input: Re// Re is the use's request of accessing resources
Output: True or Flase //True, permit; Flase, deny
Description:
1. Receive the use's request Re
2. Build query Q=?grant(Re)←c//c is authorization condition
3. DC=DEQU(c)//If c cann't be decomposed in location, send c to anthor APS
4. For each c∈DC do
5. get c's satisfaction c'
6. add c' to DCC
7. End For
8. Result=FRM(DCC)//FRM is fuzzy reasoning machine
9. If Result>μ// μ is value of authorization threshold
10. Then Return(True)
11. Else Return(Flase)
12. End If

Algorithms: DEQU

Input: c // c is authorization condition
Ouput: DC// DC is a set of decomposed result
Description:
1. If ∃r∈Rulebase and c is the premise part of r
2. Then DEQU(c)
3. Else Add c to DC
4. End If
5. Return DC

3.3 授权模糊推理器

模糊推理器 FRM 是系统的核心部件，主要功能是基于模糊访问控制规则进行模糊授权推理。图 3 给出了 FRM 的体系结构，FRM 是一个多输入单输出的模推理器，输入为多个表示条件满足程度的模糊数，输出是一个表示授权强度的模糊数。最后系统将 FRM 输出的推理结果与系统设定的安全强度阈值进行比较，如果推理结果大于当前的安全强度阈值，则授予权限；否则，拒绝授权。

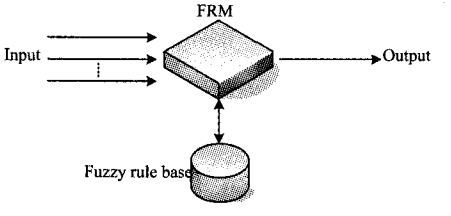

图 3 授权模糊推理器

本文首先给出了一种区间值模糊访问控制授权规则，FRM 的模糊授权推理过程都是基于区间值模糊规则进行的，然后给出了 FRM 推理计算方法。

区间值模糊集合理论早在 1975 年就被提出，近年来人们对区间值模糊集的研究兴趣与日俱增，主要原因在于实际应用中一个模糊集的隶属度往往不易确定，而区间值隶属度相对而言较易确定[19,20]。此外，模糊推理结果用区间值模糊集来表示更能反映日常推理的模糊性。因此，为了表达普适计算环境下访问控制的模糊不确定性以及访问控制策略的复杂性、动态性的特点，我们在区间值模糊集合理论基础上，提出了一种区间值模糊访问控制授权规则，用来描述模糊安全策略。其结构定义为：

$$r,\lambda: \mathrm{IF}(P_1,[x_1^-,x_1^+],w_1)\ \mathrm{and}\ (P_2,[x_2^-,x_2^+],w_2)\ \mathrm{and}\ \cdots\ \mathrm{and}\ (P_n,[x_n^-,x_n^+],w_n)\ \mathrm{THEN}\ (Q,[z^-,z^+])CF(\mu)$$

式中，r 是规则的唯一标识；λ 是规则 r 的可信度，$0\leqslant\lambda\leqslant1$，表示用规则 r 所得出推理结果的可靠程度；符号“IF”含义为“如

果”，“THEN”含义为“那么”；$(P_1,[x_1^-,x_1^+],w_1)$ and $(P_2,[x_2^-,x_2^+],w_2)$ and … and $(P_n,[x_n^-,x_n^+],w_n)$ 表示授权规则条件，其中每一个子条件用模糊谓词表示，第 $i(1\leqslant i\leqslant n)$ 个模糊谓词 P_i 表示规则 r 的第 i 个子条件，子条件可以与普适计算环境中的上下文相关也可以与上下文无关，其区间值隶属度 $[y_i^-,y_i^+]$ 表示模糊谓词 P_i 所代表的子条件的满足程度，$w_i(0\leqslant w_i\leqslant 1)$ 表示模糊谓词 P_i 在规则条件 P 中的权重，表明该模糊谓词在模糊推理过程中对推理结果的影响程度，权重越大，对推理结果的影响越大，并且 $w_1+w_2+\cdots+w_n=1$；“and”是逻辑“并且”连接词，表示规则条件 P 中的所有子条件必须得到满足；Q 是授权规则条件满足时产生的结果，$[z^-,z^+]$ 表示 Q 能够被该规则推导出来的可能性程度，也表示授权强度的程度；$CF(\mu)(0\leqslant\mu\leqslant 1)$ 表示规则条件 P 可以激活规则 r 的激活阈值，用来刻画上下文能激活规则的最小满足程度，如果上下文与规则条件的匹配度大于激活阈值，那么该规则可以被激活，否则不被激活。规则 r 的含义是：如果授权规则的每一个子条件被模糊满足，那么规则得到的授权结果即可得以模糊实施。

下面给出 FRM 推理计算方法。FRM 推理过程实际上是对普适访问控制策略模糊规则(大前提)和实际存在的与访问控制相关的事实(小前提)构成的知识库进行推理，也就是要完成下面的推理问题：

大前提：IF$(P_1,[x_1^-,x_1^+],w_1)$ and $(P_2,[x_2^-,x_2^+],w_2)$ and … and $(P_n,[x_n^-,x_n^+],w_n)$ THEN$(Q,[z^-,z^+])$ $CF(\mu)$

小前提：$(R_1,[y_1^-,y_2^+])$ and $(R_2,[y_2^-,y_2^+])$ and … and $(R_n,[y_n^-,y_n^+])$

结论：$(Q,[v^-,v^+])$

为了求解 $[v^-,v^+]$，先给出一个前件与已知的相关事实之间的模糊匹配程度的计算函数 $M(R,P)$：

$$M(R,P)=1+\frac{\sum_{i=1}^{n}(y_i^--x_i^-)w_i}{2\sum_{i=1}^{n}x_i^-}+\frac{\sum_{i=1}^{n}(y_i^+-x_i^+)w_i}{2\sum_{i=1}^{n}x_i^+} \quad (1)$$

式中，$R=\{R_1,R_2,\cdots,R_n\}$ 表示已知的相关事实，$P=\{P_1,P_2,\cdots,P_n\}$ 表示规则条件。函数 $M(R,P)$ 刻画了已知相关事实 R 与授权规则条件 P 的相似程度，其值越大，则表示越匹配。若该值大于等于规则条件 P 可以激活规则 r 的激活阈值 $CF(\mu)$，则系统就触发并执行该规则，并产生一个推理结果 Q，Q 的可信程度取值为模糊匹配函数 $M(R,P)$ 的值与 $[z^-,z^+]$ 的“乘积”。如果计算出的模糊匹配函数的值小于 $CF(\mu)$，则系统就不执行该规则。

设 $M(R,P)=\beta\geqslant CF(\mu)$，则通过模糊推理所得结果为：$[v^-,v^+]=[\beta*z^-,\beta*z^+]$。其中，符号“*”表示算数乘法运算。$[\beta*z^-,\beta*z^+]$ 表示通过规则 r 授权推理产生的授权强度。如果授权强度大于所请求访问资源的安全强度，则可以对该资源进行访问，否则不能访问。

下面通过一个简单实例来说明具体的推理计算过程。

例 2　假定系统中有以下授权规则：

Rule1　如果用户进入智能教室的可能性较大，授权请求时间为上课时间的可能性较高，请求使用设备的工作状态为比较空闲，用户在系统访问记录中评价为较好，则授予用户对请求设备使用权限的强度较高。

根据 Rule1 可以定义 5 个模糊谓词 P_1,P_2,P_3,P_4,Q，其中，P_1 表示进入智能教室，P_2 表示请求时间为上课时间，P_3 表示请求使用设备的工作状态，P_4 表示用户在系统访问记录中的评价，Q 表示授予用户对请求设备使用权限的强度，并为 P_1,P_2,P_3,P_4,Q 分别赋予表示程度的区间隶属值。设 P_1,P_2,P_3,P_4 对应的权重为 $w_1=0.3,w_2=0.7,w_3=0.4,w_4=0.3$。假设规则 1 的 $CF(\mu)$ 等于 0.6，则授权规则 1 可表示为：

r_1,λ_1：IF$(P,[0.8,0.9],0.3)$ and $(P,[0.1,0.2],0.7)$ and $(P,[0.4,0.6],0.4)$ and $(P,[0.5,0.7],0.3)$ THEN Q $[0.8,0.9]$

用户 u 和 u' 经过授权查询后，对授权条件的满足情况(匹配事实结果)分别为 R 和 R'，即

$R=(R_1,[0.8,0.9])$ and $(R_2,[0.3,0.4])$ and $(R_3,[0.1,0.2])$ and $(R_4,[0.1,0.2])$

$R'=(R_1',[0.8,0.9])$ and $(R_2',[0.7,0.8])$ and $(R_3',[0.5,0.6])$ and $(R_4',[0.3,0.4])$

根据式(1)可以计算出用户 u 和 u' 的相关事实满足情况分别与授权规则 1 的匹配结果：$M(R,P)=0.4$，$M(R',P)=0.7$ (计算过程略)。由结果可知：$M(R,P)=0.4<CF(\mu)$，$M(R',P)=0.7>CF(\mu)$。因此，用户 u' 将启动并执行规则 1，并产生推理结果：$[v^-,v^+]=0.7\times[0.8,0.9]=[0.56,0.63]$。该结果表示对用户 u' 授予权限的强度在 0.56 到 0.63 之间。这样的推理结果与通过授权规则直观判断的授权结果是吻合的。

用户通过 FRM 推理获得授予权限的强度 $[v^-,v^+]$ 后，系统将根据当前环境或资源服务器设定的访问控制安全强度 π 确定对用户的访问控制。π 表示访问控制强度，可以刻画系统安全强度随计算上下文变化的自调节性，其随环境上下文而动态变化。系统将监测 π 的变化，π 发生变化意味着系统的访问控制强度发生变化，此时需要重新判断系统授权，重新检测用户访问权限的合法性。在系统或资源服务器中可以定义访问控制规则：当用户的授权强度 $[v^-,v^+]$ 在访问控制强度 π 内时，可以授予用户权限，否则拒绝授予权限。在上面例子中，设 $\pi=[0.5,0.8]$，u' 经过推理得到的授权强度 $[v^-,v^+]=[0.56,0.63]\subset\pi$，所以 u' 可以获得请求的权限。

通过安全强度 π 的设定可以实现普适计算环境下动态的权限控制和模糊自适应访问控制。π 可以通过在模糊规则库中定义系统安全强度控制规则来进行自动控制调节，或者可以定义为一个分段函数实现。例如，在一般会议期间，智能会议室的安全强度为 $[0.1,0.3]$；在保密会议期间，智能会议室的安全强度为 $[0.6,0.8]$；在绝密会议期间，智能会议室的安全强度为 $[0.8,1]$。这里 $[1,1]$ 表示最高安全强度，$[0,0]$ 表示最低安全强度。

模糊推理器能否高效工作，与模糊规则库有很大关系。模糊推理器中的控制规则一般是基于人为经验建立的，而推理过程是严格依据规则库进行的。因此，所建立的规则库是否合理有效并具有完备性至关重要。有关模糊规则库完备性的定义和证明较为复杂，我们将另文介绍。

4　授权查询信息加密机制

由于授权查询过程是通过多个服务器分布式完成的，为了保证查询过程中信息的保密性和完整性，本节给出了一种信息加密机制。其主要思想是：在发送信息时用目标服务器的公钥对信息加密，以保证只有目标服务器才能获得正确的

授权结果。为了保证发送结果的真实性，服务器可以在发送信息时用自己的私钥对信息进行签名，以证明信息发送者的身份。我们用$(p,(value)\ Kp)$描述加密信息，其中 p 表示接收的目的服务器，$value$ 表示信息的内容，Kp 是 p 的公钥。如果要对信息用私钥 Pr 签名，可表示为$((p,(value)\ Kp))\ Pr$。下面通过一个实例来说明信息加密返回过程。

例 3　在图 4 中 $p0-p8$ 表示不同的服务器，其中 $p0$ 是 RS；$p1-p4$ 是 AS；$p5-p8$ 是 APS。$p0$ 发送的授权请求通过 $p1-p4$ 完成授权的分解工作，最后通过 $p5-p8$ 完成授权子查询的验证。图 4 中实线箭头表示授权查询信息的发送，虚线箭头表示查询验证结果信息的返回。在授权结果返回时，APS 要用目的 AS 的公钥对查询结果加密。例如图 4 中 $p5$ 完成了对查询?roleIn（wu，Tea，CDept）的验证，得到结果[0.8，0.9]（表示满足的程度是 0.8 到 0.9 之间），并要把结果[0.8，0.9]返回给 $p3$。所以在 $p5$ 发送信息时要对结果用 $p3$ 的公钥 $K3$ 加密，即发送信息$(p3,[0.7,0.8]K3)$。当 $p3$ 收到该信息后，只要用自己的私钥 $P3$ 解密，就可以得到正确的查询结果。如果 $p5$ 为了保证发送信息的真实性（即证明是自己发送的信息），$p5$ 可以用自己的私钥 $P5$ 对加密结果签名，即发送信息$((p3,[0.7,0.8]K3))P5$。$p3$ 接收信息后，先用 $p5$ 的公钥 $K5$ 确认信息是由 $p5$ 所发送的，然后再用自己的私钥 $P3$ 解密察看信息内容。

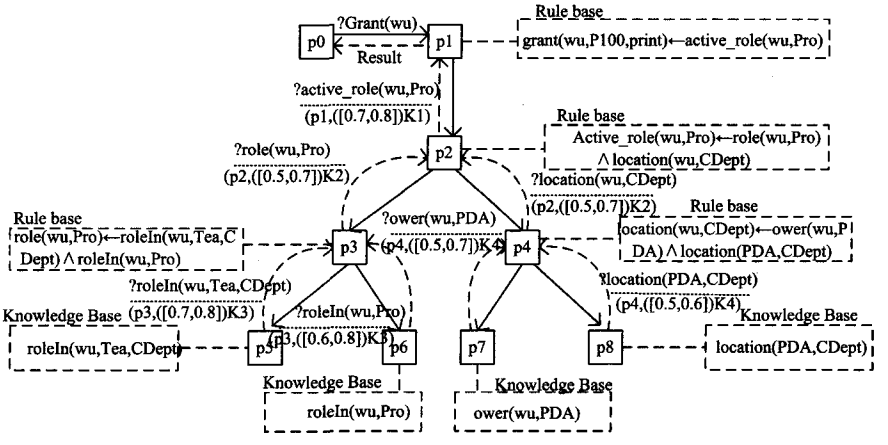

图 4　授权查询过程中的信息加密

为了防止参与授权查询的服务器被恶意监听而造成信息泄露，在返回查询结果时可以选择不同的加密策略。例如在图 4 中，假设 $p8$ 返回的结果不希望 $p4$ 获得，$p8$ 可以对结果用 $p2$ 的公钥 $K2$ 加密，发送信息$(p2,[0.5,0.6]K2)$。这样 $p4$ 收到信息，但无法查看内容，只能转发给 $p2$。如果授权查询过程中参与授权查询的服务器较多，在信息返回时有多条返回路径，采用随机选择一条路径的策略，防止某一服务器上可能存在恶意侦听。

结束语　安全问题是普适计算进一步普及应用过程中的关键问题，现有的访问控制系统不能完全适用于普适计算环境的安全需求。为此，本文针对普适计算环境的特点，提出了一个安全分布式访问控制系统 SDAC，SDAC 基于授权查询分解的思想，适用于结构分散的普适计算环境。本文还设计了一个加密机制，保证了分布式查询过程中信息的保密性和完整性。此外，SDAC 还具有模糊授权推理能力，可以根据安全策略及上下文的变化，动态调整用户权限，使得授权和访问控制自适应于普适计算环境，为智能访问控制的研究提供了新思路。

参 考 文 献

[1] Welser M. The computer of the 21'st Century[J]. Scientific American, 1991, 265(3): 66-75

[2] Michael F, Oliver R. Ubiquitous computing : An overview of technology impacts[J]. Telematics and Informatics, 2011, 28(2): 55-65

[3] Mieso K, Denko, Tao S, et al. Trust management in ubiquitous computing: A bayesin approach[J]. Computer Communications, 2010, 34(3): 398-406

[4] Jalal A M, Raquel H. Access control using threshold cryptography for ubiquitous computing environments[J]. Journal of King Saud University Computer and Information Sciences, 2011, 34(1): 1-8

[5] 林闯，封富君，李俊山. 新型网络环境下的访问控制技术[J]. 软件学报，2007，18(4)：955-966

[6] 翟浩良，韩道军，李磊. 基于情景演算的动态访问控制模型[J]. 计算机科学，2012，39(6)：35-38

[7] Youna J, James B D. CRiBAC: Community-centric role interaction based access control model[J]. Computers Security, 2012, 3(1): 497-523

[8] Rafael T, Carlos M, Altair S. Applying a usage control model in an operating system kernel[J]. Journal of Network and Computer Applications, 2011, 34(3): 1342-1352

[9] Tao W, Zhang G Q. Trusted interaction approach for dynamic service selection using multi-criteria decision making technique [J]. Knowledge Based Systmes, 2012, 32(5): 116-122

[10] 封孝生，王桢文，黎湘运. P2P 中基于信任和属性的访问控制[J]. 计算机科学，2011，38(2)：28-31

[11] Denko M K, Tao S, Issac W. Trust management in ubiquitous computing: A Bayesian approach[J]. Computer Communications, 2011, 34(2): 398-406

[12] Ding Y S, Liu F M, Tang B Y. Context-sensitive trust computing in distributed environments[J]. Knowledge Based Systems, 2012, 28(11): 105-114

[13] Bernd B. Ontology driven health information systems architectures enable pHealth for empowered patients[J]. International Journal of Medical Informatics, 2011, 80(5): 17-25

（下转第 186 页）

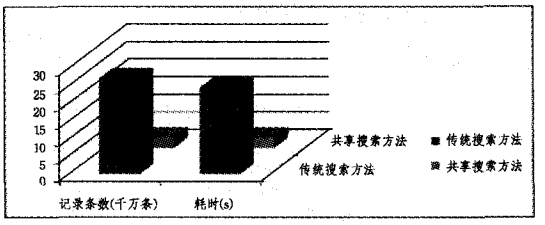

图 4　仿真实验 1 仿真结果

从图 4 可以看出，我们的搜索方法在执行搜索时需首先检查历史查询网，由于以前历史上曾经有过对包含“自行车”的搜索，因此只需要直接对新增部分的记录执行新的搜索即可，以前的记录不需要重新进行搜索，可以直接利用。图 4 的左边展示了新的搜索方法和传统的搜索方法所需要的搜索记录的一个对比，可以看出我们的搜索方法只需要搜索较少的搜索记录。图 4 的右边展示了传统搜索方法和我们的搜索方法在耗时上的一个比较，从该比较可以看出我们的搜索方法由于只需要搜索较少的记录，因此大大地减少了搜索的时间，提高了查询效率。

2)复杂查询搜索仿真实验比较

本仿真实验 2 主要是验证查询两个数据集的 Join 连接。本仿真实验直接从 TPC-H 数据集中选择了两个表进行 Join 连接复杂查询计算。仿真实验结果如图 5 和图 6 所示。

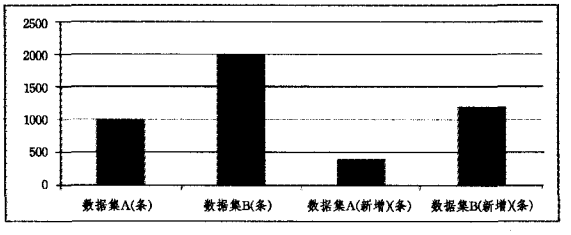

图 5　仿真实验 2 仿真结果(计算记录条数比较)

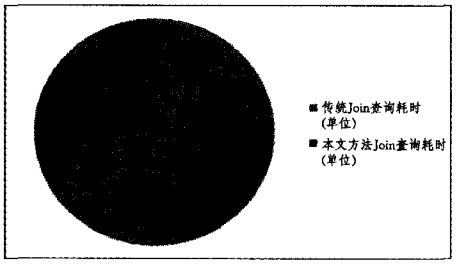

图 6　仿真实验 2 仿真结果(计算时间比较)

从图 5 和图 6 可以看出，使用本文的方法进行 Join 连接的复杂查询，无论计算记录的条数还是最后的计算所花费的时间，均有一定程度的提高。

结束语　本文针对大数据查询效率低下的问题，提出了一种有效的搜索方法。我们的主要设计思想是将共享的历史查询结果作为中间结果集，在新的查询请求到达时，首先与历史查询进行匹配，若能实现匹配，则直接将匹配部分的历史查询结果作为新查询请求结果的一部分。这减少了大量的对历史查询的重复计算，节省了搜索时间，提高了查询效率。最后通过实验对比分析得出，新的基于大数据的查询方法能较好地提高查询效率。

为了进一步提高大数据下的搜索效率，未来的工作主要集中于如下几个方面：

(1)建立一个针对大数据的语义网，增强近似查询的能力。通过语义网，可以实现语义查询的需求。

(2)改善 MapReduce 的计算能力。MapReduce 的 Shuffle 阶段一直是制约 MapReduce 计算能力的一个重要瓶颈，以后要设计一种较为灵活的 Shuffle 处理机制，从而提高其处理能力，实现更为快速高效的搜索。

参 考 文 献

[1] Dean J, Ghemawat S. MapReduce: Simplified data processing on large clusters[C]// Brewer E, Chen P, eds. Proc. of the OSDI. California: USENIX Association, 2004: 137-150

[2] Ekanayake J, Li Hui, Zhang Bing-jing, et al. Twister: A Runtime for Iterative MapReduce[C]// The First International Workshop on MapReduce and its Applications (MAPREDUCE'10). 2010: 110-119

[3] Bu Y Y, Howe B, Balazinska M, et al. HaLoop: Efficient iterative data processing on large clusters[J]. PVLDB2010, 2010, 3(1/2): 285-296

[4] Isard M, Budiu M, Yu Y, et al. Dryad: Distributed data-parallel programs from sequential building blocks[J]. ACM SIGOPS Operating Systems Review, 2007, 41(3): 59-72

[5] Zaharia M, Chowdhury M, Franklin M J, et al. Spark: Cluster Computing withWorking Sets[R]. Technology report of UC Berkeley. 2011

[6] Dittrich J, Quian'e-Ruiz J A, Jindal A, et al. Hadoop++: Making a yellow elephant run like a cheetah (without it even noticing)[J]. PVLDB, 2010, 3(1/2): 518-529

[7] 陈国华，汤庸，彭泽武，等. 基于学术社区的学术搜索引擎设计[J]. 计算机科学，2011，38(8)：171-175

[8] 殷哲，曹炬. 带差商信息的云搜索优化算法及其收敛性分析[J]. 计算机科学，2012，39(1)：252-255，267

[9] 杨艺，周元. 基于用户查询意图识别的 Web 搜索优化模型[J]. 计算机科学，2012，39(1)：264-267

(上接第 137 页)

[14] Anisetti M, Ardagna C A, Bellandi V, et al. OpenAmbient: a Pervasive Access Control Architecture[M]. Security in Autonomous Systems, 2006: 160-172

[15] Vassilis K, Loukas H, Dimitris K, et al. A dynamic context-taware access control architecture for e-services[J]. Computers Security, 2006, 25(7): 507-521

[16] Takabi, Amini, Jalili. Enhancing role-based access control model through fuzzy Relations[J]. Information Assurance and Security, 2007, 15(3): 131-136

[17] Zhang S, He D K. Fuzzy model for trust evaluation[J]. Journal of Southwest Jiaotong University, 2006, 14(1): 23-28

[18] 窦文阳，王小明，张立臣. 普适计算环境下的动态模糊访问控制模型研究[J]. 计算机科学，2010，37(9)：63-37

[19] Chen S M, Li W, Liu H C, et al. Multiattribute decision making based on interval-valued intuitionistic fuzzy values[J]. Expert System with Applications, 2012, 39(13): 343-351

[20] Sevastjanow P, Dymova L, Barosiewicz P. A new approach to normalization of interval and fuzzy weights[J]. Fuzzy Sets and Systems, 2012, 198(2): 34-45