普适环境下的基于信任度的动态模糊访问控制模型①

杨 升, 郭 磊

(武夷学院 数学与计算机学院, 武夷山 354300)

摘 要: 普适计算是国际公认的未来计算主流模式之一, 本文针对其安全性问题, 提出了普适环境下的基于信任度的动态模糊访问控制模型 TDFACM, 该模型将传统的访问控制模型与区间值模糊计算理论结合, 通过对主体信任度评估进行授权决策, 并给出了加权模糊值推理方法. 该模型能更好的解决普适环境下访问控制模型的实用性与安全性.

关键词: 普适计算; 访问控制模型; 模糊授权; 区间值模糊推理

Trust-based Dynamic Fuzzy Access Control Model in Pervasive Computing

YANG Sheng, GUO Lei

(Department of Mathematics and Computer Science, Wuyi University, Wuyishan 354300, China)

Abstract: Pervasive computing is considered as one of internationally recognized mainstreams of future computing. Trust-based Dynamic fuzzy access control model TDFACM in pervasive computing was put forward according to its security problem. This model combined traditional access control model with the theory of interval-vlaued fuzzy computing. Authorized decision will be made in accordance to the trust evaluation to the subject and the way of authorized fuzzy interference will be given as well. This mode can well solve the security and practicability of access control model in pervasive computing.

Key words: pervasive computing; access control model; fuzzy authorization; interval-vlaued fuzzy reasoning

1 引言

普适计算[1-3]是一种全新的计算模式,最早由美国 Xerox PARC 实验室的 Mark Weiser 于 1991 年提出, 它将信息空间与物理空间融合,为用户提供实时的、透明的数字化服务. 普适计算环境是非孤立的、开放的、互联的, 用户在该环境中能够在任何时间任何地点访问资源, 提供服务. 但这种无处不在的开放环境决定了普适计算环境对安全的新要求, 访问控制则是保证环境中服务与设备安全的有效方法[4,5].

目前为止, 较普遍使用的访问控制模型共有三种: DAC、MAC 与 RBAC, 学术界与工业界公认 RBAC96 系列模型相对而言比较适合普适访问控制[6,7]. 但传统的访问控制系统是针对静态网络或者封闭系统, 用户事先已经完成了登记注册, 即用户的授权管理有了明确对象. 在普适计算环境中, 资源的拥有者与请求者之间并不相识, 传统的基于身份的访问控制无法完成权限管理. 普适计算最大的特点是上下文感知, 通过用户行为来调整主体与客体属性, 这种改变必然影响到本次或下次的访问授权判断, 而传统的访问控制中, 属性只能通过管理行为才能被改变, 如此必然会给管理员带来沉重的负担, 而且普适设备的能源有限, 也无法处理由于上下文的动态变化而导致的复杂的角色变换.

本文提出了普适环境下的基于信任度的动态模糊访问控制模型 TDFACM(trust-based Dynamic fuzzy access control model in pervasive computing), 通过对用户的可信程度进行评估, 并结合区间模糊计算理论[8], 给出了用户可信任度加权模糊推理方法, 得到最终的主体信任度, 实现普适访问控制的动态模糊授权.

① 基金项目:福建省教育厅项目(JA11265);武夷学院科技项目(XQ0932)
收稿时间:2013-06-01;收到修改稿时间:2013-07-01

2 普适环境下的基于信任度的动态模糊访问控制模型

在普适计算的环境中, 我们关心的是访问主体的可靠性, 而不是用户的身份, 因此在本模型中, 将根据用户的动态变化的属性值进行计算并得到用户的信任度, 该信任度不是一个固定的值, 而是一个区间值, 再根据这个信任区间值与客体的授权阈值进行比较来决定主体授权. 图1给出了TDFACM的访问控制框图.

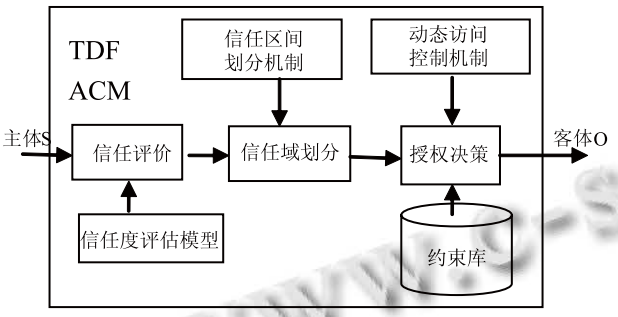

图 1 TDFACM 访问控制框图

2.1 模型元素

定义 1. 主体(Subject): 它是一类实体, 被许可进入普适计算系统, 并在满足访问控制策略的约束下对系统中的资源进行访问, 简记为 S. 在普适计算下, 主体可以是用户所在的组织(用户组)、用户本身, 也可以是用户使用的计算机终端、手机、移动设备等, 甚至可以是应用程序或进程.

定义2. 主体信任度: 系统对主体请求进行授权时的重要依据, 反映对主体的信任程度. 其值越大说明系统对其信任度越高.

定义 3. 客体(*Object*): 它是在访问控制策略约束下接受主体访问的被动实体, 简记为 O, 客体可以是硬件设备、无线终端, 也可以是系统中的文件或目录.

定义 4. 操作(*Operation*): 表示能执行的最小动作, 简记为 OP.

定义 5. 权限(*Rights*): 是主体对客体的操作的集合, 含主体对客体的作用行为和客体对主体的条件约束, 简记为 *R*. *R* 可以表示为一个四元组(*o*, *op*, *t*, *loc*), 其中 *t* 表示时间, *loc* 表示区域.

定义 6. 授权(*authorization*): 是指授权策略允许主体对特定客体执行的某些操作. 他是访问控制模型中的唯一的权限决策因素, 在执行授权过程中可能会导致主体或客体某些属性值的修改. 传统的访问控制模型中, 主体与客体访问权限之间一般只有两个值, 即允许或者不允许. 在本模型中, 对授权进行了模糊化处理, 分为了不授权, 弱授权, 部分授权, 强授权与完全授权.

定义7. 权限阈值: 每个客体的所有权限的授权都有唯一的权限阈值, 该值为对主体授权时的最小的信任度值. 当主体信任度低于权限阈值时, 拒绝授权, 当主体信任度高于权限阈值时, 同意授权.

定义8. 区间值: 表示对用户信任度评价的一个区间范围, 该值将与权限阈值进行对比以决定是否对主体进行授权. 本文中提到的区间值均为正区间值.

2.2 信任度计算机制

该模型的关键在于如何对普适计算环境中的访问实体进行信任度评估. 信任本身是带有模糊性的, 在大多数情况下, 用户评判指标往往带有不确定性, 并且知识系统中, 领域专家的评价也是通过直觉, 经验等, 其中并没有明确的逻辑关系, 专家也无法将这些知识之间的关系十分清晰的表达出来, 所以领域专家也经常使用一些含糊语言来对其进行描述. 为了更加满足普适环境下对访问控制的要求, 本模型在授权过程中也具有模糊性, 系统将会根据模糊评判分析结果对用户进行授权管理.

在主体访问系统资源前, 授权方必须获得主体的必要信息, 也可通过专用设备, 如监视器等获得主体的相关信息, 如时间、位置等. 假设目前有四个主体向系统提出访问资源的要求, 则它们的信任度的模糊评价过程如下:

设四个评价主体因素的评价指标集 $P=\{p_1, p_2, p_3, p_4\}$与权重集 $A=\{a_1, a_2, a_3, a_4\}$的值分别为:

p_1: 主体技能, 权重值 $a_1=0.3$

p_2: 主体学历, 权重值 $a_2=0.2$

p_3: 社会地位, 权重值 $a_3=0.25$

p_4: 历史信誉度, 权重值 $a_4=0.25$

各个指标对最终用户授权的结果影响并不相同, 故需根据实际情况对评价指标权重进行适当调整, 但总体权重值满足 $a_1+a_2+a_3+a_4=1$. 在这里建立评判集 $W=\{w_1, w_2, w_3, w_4\}$, w_i表示 0-100 之间的模糊集, 建立评判矩阵, 并根据模糊集理论[9], 建立因素与主体之间的隶属函数, 该函数是主体信任度与用户评价值之间的一个非负函数, 主体用模糊关系矩阵 $R=\{r_{ij}\}_{4*4}$ 表示, t 为用户指标通过专家的评价所得到的评价得分,

设建立 4 项因素的隶属函数为:

$$W_1(t)=\begin{cases}1, & 0\le t\le 50\\ \dfrac{70-t}{20} & 50\le t\le 70\\ 0 & 70\le t\le 100\end{cases}$$

$$W_2(t)=\begin{cases}0, & 0\le t\le 60\\ \dfrac{t-60}{20} & 60\le t\le 80\\ 1 & 80\le t\le 90\\ \dfrac{100-t}{10} & 90\le t\le 100\end{cases}$$

$$W_3(t)=\begin{cases}0, & 0\le t\le 20\\ \dfrac{t-50}{30} & 20\le t\le 50\\ 1 & 60\le t\le 80\\ \dfrac{100-t}{20} & 80\le t\le 100\end{cases}$$

$$W_4(t)=\begin{cases}0, & 0\le t\le 40\\ \dfrac{t-40}{20} & 40\le t\le 60\\ 1 & 60\le t\le 80\\ \dfrac{100-t}{20} & 80\le t\le 100\end{cases}$$

此处定义的隶属函数可根据实际应用中的评价等级由系统管理员进行调整. 设对Rose和Bob两人进行授权, 由专家打分的方法对Rose与Bob的四项指标评价得分情况如表 1.

表 1　综合评价表

指标	Rose	Bob
P_1	75-78	83-87
P_2	74-76	72-74
P_3	77-79	80-83
P_4	84-87	76-79

以 Rose 为例, 将 Rose 关于 $p1$ 的得分[75-78]分别代入隶属函数中,得到 Rose 在指标 $p1$ 上的为(0,[0.75, 0.9], [0.83,0.93],1), 依次将 Rose 的其余四项指标均代入函数计算, 就可得到 Rose 的模糊综合评价矩阵:

$$R_{Rose}=\begin{bmatrix}0 & [0.75,0.9] & [0.83,0.93] & 1\\ 0 & [0.7,0.8] & [0.8,0.86] & 1\\ 0 & [0.85,0.95] & [0.9,0.96] & 1\\ 0 & 1 & 1 & [0.8,0.85]\end{bmatrix}$$

由于每个指标对授权最终判断结果影响力有差异, 用加权平均模型做矩阵乘法:

A●R_{Rose} = (0,[0.8275,0.9175],[0.884,0.941],[0.95,0.9625])

为了得到每个评价再整个评价体系中的比重, 做两步计算, 首先将此矩阵的每项的左右区间值求和, 得到 Ω_{Rose}=[2.6615,2.821], 再做平均加权法, 使 A●R_{Rose} 变为 B_{Rose}=(0,[0.2933,0.3447],[0.3134,0.3536], [0.3368,0.3616]), 依据各区间值进行比较, 发现其中最大的区间为[0.3368, 0.3616], 所以 Rose 的最终信任区间值为[0.3368, 0.3616].

2.3 授权实现

TDFACM 模型的系统体系结构主要由访问控制引擎、用户知识库、监视器等几个部分构成, 其中访问控制引擎是核心部件, 主要处理用户请求与用户间的互操作; 用户知识库存储了主体、客体的属性及最新环境上下文信息; 监视器则实时监控主体、客体上下文信息, 并实时对知识库进行维护.

当问控制引擎在授权决策过程中, 若主体的信任度高于某一级别授权的权限阈值, 则可以对该主体进行授权, 若主体信任度低于最低权限阈值, 则拒绝该主体请求. 若主体的信任度处于两个区间之间, 即使跨区间的, 则分别计算该主体信任度与两个信任区间的距离, 取距离较近的区间做为其授权级别. 具体的计算公式为, 对于两个信任区间分别为[a1,a2]、[b1,b2], 则他们之间的距离公式为:

$$\Delta=\sqrt{(a1-a2)^2+(b1-b2)^2}$$

若授权级别及信任域关系如表 2.

表 2　信任域分布表

授权级别	信任域区间	描述
完全授权	[0.65，1.0]	完全信任
强授权	[0.437，0.65]	非常信任
部分授权	[0.375，0.437]	比较信任
弱授权	[0.25，0.375]	基本信任
不授权	[0，0.25]	不信任

则 Rosed 的最后授权级别为弱授权, 描述为基本信任. 具体的授权级别与信任区间的映射可根据实际情况进行设置与调整.

同时为了适应信任度的动态变化, 采用了信任度衰减机制. 即在主体较长时间没有做任何操作时, 适当对其信任度进行调整. 可设信任度调整时间阈值为 x 天, 主体在 x 天内无任何操作, 则将其授权级别调低一级.

2.4 模型应用

基于普适计算的智能教室为用户提供高效、透明、移动的办公环境. 当教师进入到特定教室, 智能系统能根据用户行为提供服务, 并根据用户上下文信息进行权限调整.

如教师 A 在上课时间进入教师, 则自动为用户开启多媒体设备, 若教师 B 收教师 A 委托进入, 则需根据教师 B 的信任度、教师 A 委托授权的信任度评价值等, 对教师 B 进行模糊授权推理, 并计算该次访问信任度区间值, 若高于教室权限阈值, 则开启相应设备, 否则拒绝请求.

该模型有几个优点, 首先, 该授权推理过程简单, 计算复杂度小, 易在通用设备, 尤其是手持式设备上使用; 其次, 对象信任度值采用区间值表示, 而对上下文信息要求也是模糊的, 更符合普适计算环境; 最后, 该推理过程充分考虑的上下文信息的实时调整, 为每个评价值设置权重, 让整个模块更具有动态性.

3 总结

普适计算目前已经成为一个研究热点, 而且传统的分布式计算的安全机制并不完全适合于普适计算. 本文结合访问控制技术, 提出了基于信任度的动态模糊访问控制模型 TDFACM, 针对信任度描述模糊性的特点, 采用区间模糊理论对主体信任度进行评估, 建立了信任度的模糊计算模型与授权模型, 并提出了信任度衰减机制. 可以看出, 通过模糊评判, 模糊决策对用户进行授权的机制, 能更好的反应实际情况, 体现访问控制的公平性, 也更能保证高级别的用户可优先使用资源. 在今后的工作中, 将进一步完善模型, 如结合检测器对用户行为进行评估, 建立多级安全评估模型, 确保安全授权.

参考文献

1 Weiser M. The computer for the twenty-first century. Scientific American, 1991, 265(3): 94–104.

2 Sakamura K, Koshizuka N. The eron wide-area distributed-system architecture for Ecommerce. IEEE Micro, 2001, 21(6): 7–12.

3 Zhang D, Chen E, Shi YC, et al. A kind of smart space for remote real-time interactive learning based on pervasive computing model. Lecture Notes in Computer Science, 2003, 2783: 297–307.

4 郭亚军,洪帆,沈海波等.普适计算面临的安全挑战.计算机科学,2007,34(6):1–3,12.

5 Bertino E, Bonatti PA, Ferrari E. TRBAC: A temporal role-based access control model. ACM Trans. on Information and System Security, 2001, 4(3): 191–223.

6 Bertino F, Gatania B, Dam I. GEO-RBAC: a spatially aware RBAC. 10th ACM Symposium on Access Control Models and Technologies. Sweden. ACM. 2005. 29–37.

7 Toahchoodee M. Access Control Model for Pervasive Computing Environments. Fort Collins, USA. Cokorado State University. 2010.

8 吴茜,叶永升,李苑青.基于区间值加权模糊推理的访问控制模型.计算机应用研究,2012,29(10):3842–3845.

9 张海娟.普适计算环境下基于信任的模糊访问控制模型.计算机工程与应,2009,45(27):107–112.

(上接第 121 页)

algorithm for multiprocessor real-time systems. IEEE Trans. on Parallel and Distributed Systems, 1998, 9(3): 312–319.

5 乔颖,王宏安,戴国忠.一种新的实时多处理器系统的动态调度算法.软件学报,2002,13(1):51–58.

6 李建国,陈松乔,鲁志辉.实时异构系统的动态分批优化调度算法.计算机学报,2006,29(6):976–984.

7 Kumar A. A modified method for solving the unbalanced assignment problems. Applied Mathematics and Computation, 2006, 176(1): 76–82.