基于 XACML 的网格访问控制研究①

Research on Grid Access Control Based on XACML

黄 刚 (南京邮电大学 江苏南京 210003)
王汝传 (南京邮电大学 江苏南京 210003)
(南京大学 江苏南京 210093)

摘要:网格的访问控制可以解决网格环境下的信息共享,通过创建策略和规则,XACML 提供了控制信息访问的机制。应用 XACML 作为网格策略表达,提出了网格访问控制的策略决策模型。在分析决策模型基础上,给出了基于 XACML 的 RBAC 网格访问控制模型,描述了使用 XACML 实现 RBAC 模型的基本方法。

关键词:网格 访问控制 XACML

1 引言

网格是将分布在不同地理位置上的异构资源通过高速网络互联起来以实现充分共享的资源集合,形成一台巨大的虚拟计算机,以提供高性能计算、管理及服务。网格中的访问控制策略既要考虑到本地的访问控制策略,又需要实现全局的访问控制,这就需要全局的访问策略和本地的访问策略进行协调和交互。目前主要的访问控制有自主访问控制和强制访问控制。在总结前人研究成果的基础上,由 Ferraiolo 和 Kuhn 在 1992 年提出的基于角色的访问控制 (Role – Based Access Control RBAC)。如何保障基于网格的访问控制已成为实施 RBAC 系统的一个重要问题。可扩展访问控制标记语言 (eXtensible Access Control Markup Language XACML) 是一个 OASIS 标准,该标准是一个通用的访问策略定义语言,提供一套语法来管理对系统资源的访问。该策略描述语言用于定义通用的访问控制需求,包括若干标准扩展点来定义新的功能、数据类型和组合逻辑等。XACML 提供了创建策略和规则来控制信息访问的机制,具有很强的访问控制策略描述能力,使用 XACML 实现基于角色的网格访问控制,将极大地增加 RBAC 系统的灵活性、扩展性和跨平台性。

2 XACML 技术

XACML 是一种通用的访问控制策略语言。它提供了请求主体(用户) 与请求目标(资源) 的行为(请求) 规则的语法 (eXtensible Markup Language XML)。XACML 对访问控制策略语言和请求/响应两方面都进行了描述。一个请求消息包含策略决策点进行访问控制决策所必须的属性信息,包括主体属性的子集、行为的属性、所请求资源的属性及执行环境的属性集。策略决策点会根据一组策略对该请求消息进行评估[1]。一个策略有两部分组成: 一个目标和一组规则。目标就是策略实施的对象,而规则是规定请求者提供的属性进行运算的规则。对于访问控制决策可能需要多重策略和规则,XACML 定义了许多规则组合算法,从而把多个决策结果组合得到一个结果。

当前绝大多数访问控制和授权系统都实现了专用的、简化的模型,通常遵循如下模式:1) 处于特定环境中的主体首先向系统发出请求;2) 系统随后检查其资料库,并为该请求授权,或拒绝该请求。资料库中包含目标资源信息、主体信息和主体可能隶属的组的信息。所有这些信息都存储在资料库中,并总称为访问控制列表。随着时间的推移,人们以各种方式实现了各种解决方案,由于安全性的问题,某些解决方案尚不完善,过于简单,这就需要使用新的技术来弥补,而 XACML 就是这样一种技术。

XACML 提供的架构具有以下优点:1) 首先,XACML 提供了可移植、统一的方法,用以描述这些访问控制元

① 基金项目:国家自然科学基金(60173037,70271050)

素，便于网格系统中的跨域访问需求；2）其次，XACML 提供了标准格式，以便于在不同系统间交换安全控制信息。这尤其利于在网格这种异构的系统之间交换安全信息；3）最后，XACML 这种标准格式也使得我们可以将原来孤立的访问控制列表联合起来，提供统一的列表信息。这有利于组织、管理、控制和监控其资产，并同时已更好的方式调节各个实体，从而有效地使用这些资产。

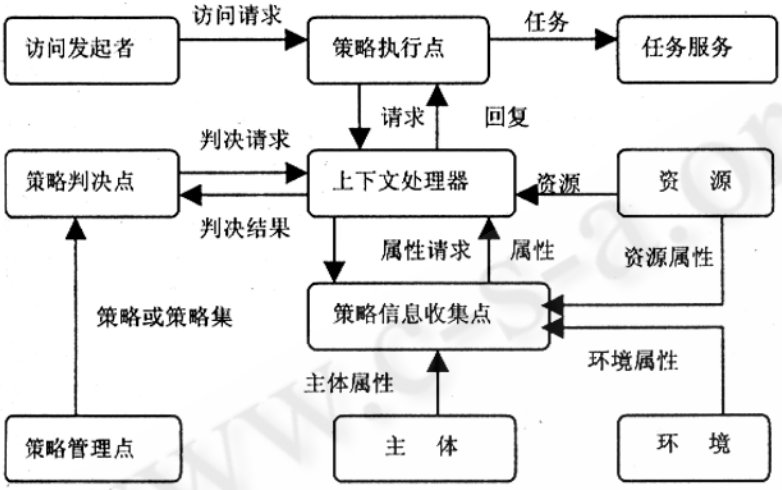

图 1　XACML 访问控制决策模型

3　基于 XACML 的网格访问决策控制模型

研究安全系统的组织建议在访问控制、数字权限管理、认证以及授权系统上使用基于的语言来描述规则。其中，XACML 是一个适用于描述分布式系统访问控制规则的语言，它得到了大量商业公司的支持。XACML 具备可扩展性，支持参数化的策略描述和多样化的策略组合。对于我们而言，XACML 语言的最具吸引力的一个特点是它能够融入简单对象访问协议调用时使用的结构中。就这一点，对 XACML 对网格的访问控制系统非常适用。与以往的策略描述语言相比，具有能够同时被人和计算机识别的特点。当然，XACML 也有其他策略描述语言同样的要素，访问目标、主体、操作以及规则等。除了给出策略的描述语法之外，XACML 也给出了一个标准化的访问控制决策模型。也就是说，XACML 的应用能够对资源的访问请求进行决策[2]。图 1 给出了的访问控制决策模型。

整个 XACML 的访问控制决策模型由若干个功能块构成。访问发起者发起访问请求。策略执行点将接收到的访问请求转发给上下文处理器。上下文处理器向策略信息收集点提出属性请求。策略信息收集点从主体、资源、环境功能块获取相关属性，返回给上下文处理器。上下文将这些属性和资源信息以及请求信息做一定的处理，向策略判决点提出包含必要信息的决策请求。策略判决点根据策略管理点提供的策略依照既定的逻辑对该决策请求做出判决，并返回判决结果。接着上下文处理器将结果返回策略执行点，由策略执行点来实施决策结果，向任务服务提交任务要求还是拒绝用户请求。显然，XACML 对的网格访问控制系统非常适用。

XACML 应用于网格访问控制具有以下特征：1）属于应用层访问控制；2）网格的基础设施和各种服务都以网格服务的方式提供，成为客户利用这些应用首先可获得的资源，需要对其进行控制；3）随着 XML 的发展，网格上的大量资源表现为以 XML 文档的形式描述。网格服务提供了一种对这些 XML 文档进行操作和共享的手段，从应用逻辑上来讲存在着层次关系。对网格资源的安全访问控制需要按照网格服务和 XML 文档资源在应用上的逻辑关系，将两者有机地结合起来；4）作为现实世界应用模式在网格世界的映射，网格资源的访问能控制需要灵活多样的访问策略描述，以更好地与现实世界中的应用相匹配。

另外，访问控制本身尚有如下要求：1）一致性：即对资源控制无二义性，各定义之间无冲突；2）统一性：对网格服务和 XML 文档进行集中管理，统一贯彻安全政策；3）细粒度的访问控制：访问控制策略应支持各种粒度水平的访问控制，包括网格服务、整个 XML 文档和文档中的单个元素；4）透明性：访问控制系统操作必须对访问请求尽可能透明。即请求者不应知道他所请求的信息是通过访问控制系统隐藏在其后的；5）无缝性：无缝的与已存在的用户认证（如数字证书）等其他安全服务相集成。访问控制必须利用数字签名完成标记级水平的访问控制[3]。

通过上述分析可以看出，XACML 是处在应用层针对各类资源的访问控制，所要控制的资源主要是网格资源服务和 XML 文档。其中这两类控制既可以很好的结合在一起，又各自相对独立。另外，在实施访问控制时，要求 XACML 能够有效的授权、细粒度的访问控

制，对访问请求尽可能透明以及无缝的与认证技术相结合。最后，通过在访问控制策略中加入临时授权以及 RBAC 相应约束机制的描述来实现更加灵活的访问策略，以满足更多网格用户应用的需求。

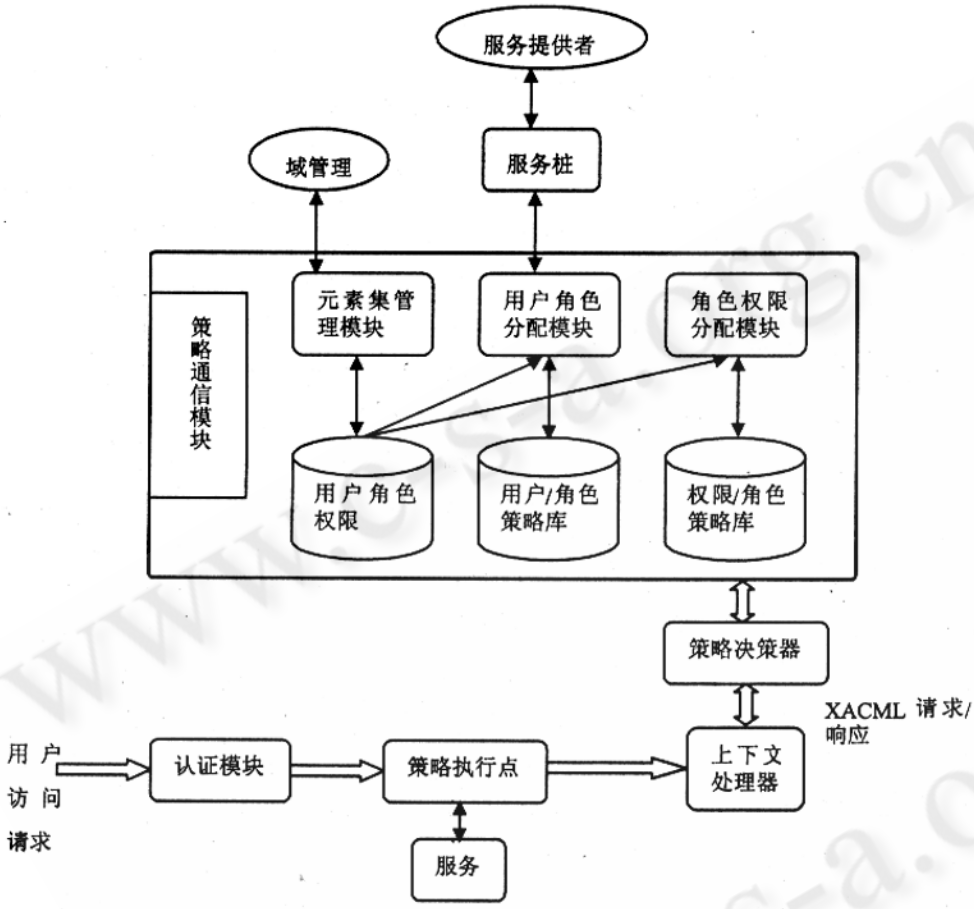

图 2　应用 XACML 的基于角色的网格访问控制模型

4　应用 XACML 的 RBAC 网格访问控制模型

根据网格访问控制的要求，提出了基于角色的网格访问控制模型如图 2 所示，该模型包括四个部分：域策略管理器，策略决策器，策略执行器，上下文处理器[4]。策略管理器有 RBAC 的四个功能子模块组成：元素集管理子模块，用户角色分配子模块，角色权限分配子模块和策略通信子模块。

元素配置管理模块以域为基础，每个域都有一个元素配置管理模块。在 NIST 的定义中，用户，角色，操作和对象是四个基本的元素。这四个元素可以被分为两类：操作与对象，用户与角色。操作与对象是相对静态的，当 RBAC 系统在某一资源或服务上配置时，操作与对象可以预定义。用户设置和角色配置却是相对动态的。

用户角色分配子模块提供用户角色配置功能，由域管理员配置与维护。用户角色配置策略存储于用户角色配置数据库。角色权限分配子模块提供角色权限配置功能，由域管理员配置与维护。角色权限策略存储于角色权限配置数据库。策略通信模块主要是用于模块之间的策略通信，包括域间角色的映射，策略消息队列与通知机制。上下文管理器用于把请求转换为 XACML 规范的形式和把 XACML 中的授权决定转换为本地化的响应。XACML 使这两种转换变得简单，灵活表达，和易于在多种环境下执行的访问控制策略。

5　使用 XACML 实现 RBAC 模型

5.1　核心 RBAC 的实现

核心 RBAC 构件是任何 RBAC 系统都必须具备的基本需求，它包含 5 个基本元素：用户、角色、对象、操作和访问权限[5]。XACML 策略可以表示 RBAC 构件，其对应关系如表 1。

访问权限可以用 XACML 的角色策略集（Role Policy Set RPS）和访问权限策略集（Permission PolicySet PPS）来表示。RPS 是一种与给定的角色属性的持有者相关的策略集，包含与给定的角色相关的实际 PPS。RPS 的目标元素限制了策略集在主体所具有的给定的角色属性的范围内：每一个 RPS 引用一个相应的访问权限策略集，但是不包含其他策略或策略集中的元素。PPS 包含与给定的角色相关的实际的访问权限的策略

集[6]。它包含 <策略> 元素和 <规则>，描述主体允许访问的资源和操作，还有有关访问发生的条件。

表 1　RBAC 构件与 XACML 元素对应关系

RBAC 构件	XACML 元素
用户	Subject
角色	Subject Attributes
对象	Resource
操作	Action
访问权限	RPS、PPS

核心 RBAC 要求对每个角色多个用户，每个用户多个角色，每角色多个访问权限和每访问权限多个角色的支持。对这里的每一个要求都可以由 XACML 策略来满足。XACML 允许多个主体与一个给定的角色属性相关。基于所拥有的特定角色的属性 <Attribute> 和属性值 <AttributeValue> 定义的 XACML RPS 能够应用于任何有请求的用户，只要角色的属性和属性值在 XACML 的请求上下文之内。XACML 允许多角色属性和一个给定的主体相关。如果一个主体有多个角色可用，那么任意的 RPS 实例应用于这其中任意一个角色都可以被评测，相应的 PPS 中的访问权限会被允许。任意角色 A 在与角色 A 相关的 PPS 中包括一个用于 PPS B 的 <PolicySetIdReference>，就可以和 PPS B 相联系。用这种方法，同样的权限集合可以和多个角色相关联。

5.2　层次 RBAC 的实现

为了满足层次 RBAC 的要求，在 XACML 中定义了上级和下级角色的概念。在角色层次中，如果角色 B 继承了角色 A 的所有的访问权限，那就称角色 A 是角色 B 的下级角色；称角色 B 是角色 A 的上级角色。XACML 策略可以这样实现角色的层次，通过在一个角色的 PPS 中包含与另一个角色相关的 PPS 的 <PolicySetIdReference>，具有 <PolicySetIdReference> 的角色也就继承了另一个角色的访问权限。因此使用 XACML 后，层次特性可以在任何时候被加到角色中，而不需要改变与其他角色相关的策略集。

5.3　职责分离的实现

在 RBAC 中引入了两种职责分离机制：静态职责分离和动态职责分离，通过 XACML 策略集可以分别解决这两种职责分离问题。职责分离策略集（Separation of Duty <PolicySet>）定义了在一个给定主体角色上的限制集合，这个策略集包含了策略和规则元素来指明角色集的限制。职责分离策略集也包含了引用到的所有角色策略集，这些实例是职责分离限制的对象。角色分配策略集（RoleAssignment <Policy> or <PolicySet>）定义了哪个角色可以被使用或可以分配给哪个主体的策略集，它指明了角色的绑定或在一个给定的主体上可以使用或可以分配的角色的数目限制。这种类型的策略可以被分配角色属性给用户的实体使用，或被在一个用户会话中激活角色属性的实体使用。

6　结束语

网格访问控制是网格计算中解决安全问题的关键技术，因网格环境的分布式、异构性、不可控制等特点，网格的访问控制必须建立在现有的访问控制系统之上。XACML 的应用能够对访问控制进行决策，并能弥补了系统的安全性问题。通过将传统 RBAC 访问控制技术和 XACML 的网格访问控制策略相结合，提出了一种基于 XACML 的 RBAC 网格访问控制模型。使用 XACML 使网格访问控制表达灵活，易于在网格环境下执行访问控制策略，使系统安全性、可扩展性、互操作性等特点。进一步的研究将能真正地实现网格访问控制的安全机制。

参考文献

1　杨宏伟、李晶、虞淑瑶、宋成，一种基于 XACML 访问控制策略决策服务的安全模型[J]，微电子学与计算机，2005，22(8).

2　高扬、张家钰、吴敏，基于 XACML 和 RBAC 的访问控制系统[J]，计算机应用与软件，2006，23(8).

3　王杨、林涛、王汝传，计算网格中访问控制策略研究与应用[J]，计算机技术与发展，2006，16(8).

4　Hai Jin, Weizhong Qiang, Xuanhua Shi and Deqing Zou ,RB－GACA: A RBAC based grid access control architecture, Int. J. Grid and Utility Computing, Vol. 1, No. 1, 2005.

5　邹晓，基于角色的访问控制模型分析与实现[J]，微计算机信息，2006，22(6－3).

6　彭军、徐燕、高阳等，基于 XML 和 XACML 的角色访问控制的实施[J]，石河子大学学报，2005，23(2).