[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480021900.9

[45] 授权公告日 2008 年 1 月 9 日

[11] 授权公告号 CN 100361037C

[22] 申请日 2004.4.23
[21] 申请号 200480021900.9
[30] 优先权
[32] 2003. 6. 5 [33] US [31] 10/455,165
[86] 国际申请 PCT/EP2004/005185 2004.4.23
[87] 国际公布 WO2004/109480 英 2004.12.16
[85] 进入国家阶段日期 2006.1.27
[73] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 朱利安尼·F.·霍
[56] 参考文献
US5335346A 1994.8.2
US5129083A 1992.7.7
审查员 孟宪超

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 康建峰

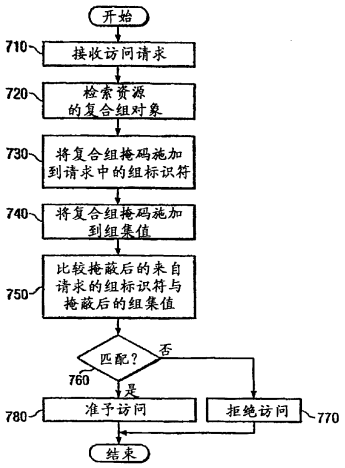
权利要求书 2 页 说明书 14 页 附图 4 页

[54] 发明名称

用于在数据处理系统中认证访问请求的方法与装置

[57] 摘要

本发明提供一种用于将多个安全组表示为单个数据对象的系统和方法。 通过该系统和方法，创建由组集值和掩码值组成的复合组对象。 复合组对象通过组集值表示多个组。 掩码值用来施加到在认证处理期间接收的组标识符，以生成与组集值相比较的值，从而确定组标识符是否是复合组的一部分。例如，在授权处理的第一步骤中，将在授权请求中接收的组标识符与复合组数据对象的掩码值进行按位求与。 在第二步骤中，将掩蔽后的来自所接收请求的组标识符与复合组对象的组集值相比较。 该比较可以采取这样的形式，即掩蔽组集值，并且将掩蔽后的组集值与掩蔽后的来自所接收请求的组标识符相比较。 如果这两个值相匹配，则准予访问。如果这两个值不匹配，则拒绝访问。



1. 一种在数据处理系统中认证访问请求的方法，包括:

接收访问请求，其中访问请求包括组标识符，并且指定被请求访问的资源;

检索与资源相关联的复合组数据对象，其中复合组数据对象包括表示多个请求者组的组集值和掩码值;

将掩码值施加到组标识符，以生成掩蔽后的组标识符;

将掩码值施加到组集值，以生成掩蔽后的组集值；以及

比较掩蔽后的组标识符与掩蔽后的组集值，并根据比较结果认证访问请求。

2. 如权利要求 1 所述的方法，其中如果掩蔽后的组标识符匹配掩蔽后的组集值，则授权访问请求。

3. 如权利要求 1 所述的方法，其中如果掩蔽后的组标识符不匹配掩蔽后的组集值，则拒绝访问请求。

4. 如权利要求 1 所述的方法，其中将掩码值施加到组标识符包括对掩码值和组标识符进行按位求与。

5. 如权利要求 1 所述的方法，其中将掩码值施加到组集值包括对掩码值和组集值进行按位求与。

6. 如权利要求 1 所述的方法，其中掩码值是分级组成员关系掩码值、组类别成员关系掩码值、以及混合掩码值之一。

7. 一种用于在数据处理系统中认证访问请求的装置，包括:

用于接收访问请求的部件，其中访问请求包括组标识符，并且指定被请求访问的资源;

用于检索与资源相关联的复合组数据对象的部件，其中复合组数据对象包括表示多个请求者组的组集值和掩码值;

用于将掩码值施加到组标识符以生成掩蔽后的组标识符的部件;

用于将掩码值施加到组集值以生成掩蔽后的组集值的部件；以及

用于比较掩蔽后的组标识符与掩蔽后的组集值并根据比较结果认证

访问请求的部件。

8. 如权利要求 7 所述的装置，其中如果掩蔽后的组标识符匹配掩蔽后的组集值，则授权访问请求。

9. 如权利要求 7 所述的装置，其中如果掩蔽后的组标识符不匹配掩蔽后的组集值，则拒绝访问请求。

10. 如权利要求 7 所述的装置，其中用于将掩码值施加到组标识符的部件包括用于对掩码值和组标识符进行按位求与的部件。

11. 如权利要求 7 所述的装置，其中用于将掩码值施加到组集值的部件包括用于对掩码值和组集值进行按位求与的部件。

12. 如权利要求 7 所述的装置，其中掩码值是分级组成员关系掩码值、组类别成员关系掩码值、以及混合掩码值之一。

用于在数据处理系统中认证访问请求的方法与装置

技术领域

本发明涉及一种用于将多个安全组表示为单个数据对象的系统和方法。更具体地说，本发明涉及一种用于使用复合组值(complex group value)和掩码值(mask value)来表示和认证多个安全组的机制。

背景技术

在大多数大规模计算系统中，用户和资源典型地以组安排，以便管理系统安全。例如，可以提供访问控制列表，以便管理由计算系统的其它资源和/或用户对资源的访问。访问控制列表是与文件、目录或其它资源相关联的一组数据，其定义用户、组、处理(process)或设备所具有以便访问它的权限。例如，可以为“管理员”建立组，并且可以将用户的标识符添加到该组，以指定该用户为“管理员”。如果资源的访问控制列表指示了只能向“管理员”提供对资源的访问，则其标识符属于“管理员”组的用户将能够访问该资源。

很多大型计算系统的一个问题是计算机系统中的组标识符的激增。当用户或资源请求对另一个资源的访问时，平均起来，认证必须遍历整个组列表的一半，以识别与请求访问的用户或资源相关联的组，然后确定是否存在访问权限。也就是，随着在计算机系统中所使用的组数增加，执行认证处理所需的时间也增加。这导致了计算机系统的性能的降低。

这样，具有一种用于以确定是否准许对资源的访问无需遍历较大的组标识符列表的方式表示用户/资源组的系统和方法将是有利的。

发明内容

本发明提供了一种用于将多个安全组表示为单个数据对象的系统和方法。通过本发明的系统和方法，创建由组集值和掩码值组成的复合组对象。复合组对象通过组集值表示多个组。掩码值用来施加到在认证处理期间接收的组标识符，以生成与组集值相比较的值，从而确定组标识符是否是复合组的一部分。

例如，本发明的授权处理是两步骤操作。在该处理的第一步骤中，将在授权请求中接收的组标识符与复合组的掩码值进行按位求与。在第二步骤中，将掩蔽(mask)后的来自所接收请求的组标识符与复合组对象的组集值相比较。例如，该比较可以采取这样的形式，即掩蔽组集值，并且将掩蔽后的组集值与掩蔽后的来自所接收请求的组标识符相比较。如果这两个值相匹配，则准予访问。如果这两个值不匹配，则拒绝访问。

这样，通过本发明，可以使用相同的组集值来表示多个不同组。可以向多个资源提供不同的掩码值，以便识别组集值中的哪些组被授权访问相关资源。结果，可以向多个资源提供复合组对象，其全都具有相同的组集值，但是可以针对它们的特定目的而具有不同的掩码值。

通过本发明，授权对给定资源的访问所需的处理量保持相同，而与组数无关。可以通过增加组集值和掩码值中的位数来增加另外的组。然而，授权处理将总是由这样的两步骤处理组成，即对所接收的组标识符进行掩蔽，并且将掩蔽后的组标识符与资源的复合组对象的组集值相比较。换句话说，由计算系统维护的“组”结构的大小不会显著地影响本发明的授权处理的性能。

本发明的这些和其它特性和优点将在下面对优选实施例的详细描述中加以描述，或者根据下面详细描述，它们对于本领域的普通技术人员而言将会变得清楚。

附图说明

被认为是本发明特征的新颖特性在所附权利要求中加以阐述。然而，通过参考下面结合附图阅读的对说明性实施例的详细描述，将最佳

地理解本发明本身以及优选使用方式及其另外的目的和优点，其中：

图 1 是可以实现本发明的分布式数据处理环境的示例图；

图 2 是可以实现本发明的服务器计算设备的示例图；

图 3 是可以实现本发明的客户端或独立计算设备的示例图；

图 4 是根据本发明实施例的复合组数据对象的示例图；

图 5 是示出根据本发明示例性实施例的数据流的示例图；

图 6 是可以与本发明的实施例一起使用的组集值和各种掩码值的示例图；以及

图 7 是概述本发明一个实施例的示例性操作的流程图。

具体实施方式

本发明提供了一种用于基于表示多个用户/资源组的单个数据对象而认证资源访问请求的机制。本发明优选地在分布式数据处理环境中实现，其中存在可以通过一个或多个网络访问该分布式数据处理环境的资源的多个用户/资源组。然而，本发明也可以在独立计算设备中实现。因此，提供图 1-3 中的下图是为了提供用于随后描述本发明的操作的上下文。

现在参照附图，图 1 示出了可以实现本发明的数据处理系统的网络的图示。网络数据处理系统 100 是可以实现本发明的计算机网络。网络数据处理系统 100 包含网络 102，其是用来在网络数据处理系统 100 内连接在一起的各个设备和计算机之间提供通信链路的介质。网络 102 可以包括诸如有线、无线通信链路或光纤缆线的连接。

在所示例子中，服务器 104 与存储单元 106 一起连接到网络 102。另外，客户端 108、110 和 112 连接到网络 102。这些客户端 108、110 和 112 可以例如是个人计算机或网络计算机。在所示例子中，服务器 104 向客户端 108-112 提供数据，例如引导文件、操作系统映象、以及应用程序。客户端 108、110 和 112 是服务器 104 的客户端。网络数据处理系统 100 可以包括未示出的另外服务器、客户端、以及其它设备。在所示例子中，网络数据处理系统 100 是因特网，其中网络 102 表示使

用传输控制协议/网际协议(TCP/IP)协议集以便相互通信的网络和网关的全球集合。因特网的心脏处是主节点或主机计算机之间的高速数据通信线的中枢，其由成千上万的传送数据和消息的商业、政府、教育和其它计算机系统组成。当然，网络数据处理系统 100 也可以被实现为多种不同类型的网络，例如内联网、局域网(LAN)或广域网(WAN)。图 1 旨在作为示例，而不作为本发明的架构限制。

参照图 2，示出了根据本发明优选实施例的可以作为服务器如图 1 中的服务器 104 而实现的数据处理系统的方框图。数据处理系统 200 可以是对称多处理器(SMP)系统，其包括连接到系统总线 206 的多个处理器 202 和 204。可选地，可以采用单处理器系统。另外，连接到系统总线 206 的是存储器控制器/高速缓存 208，其向本地存储器 209 提供接口。I/O 总线桥 210 连接到系统总线 206，并且向 I/O 总线 212 提供接口。存储器控制器/高速缓存 208 和 I/O 总线桥 210 可以如图所示集成在一起。

连接到 I/O 总线 212 的外围组件互连(PCI)总线桥 214 向 PCI 本地总线 216 提供接口。多个调制解调器可以连接到 PCI 本地总线 216。典型的 PCI 总线实现将支持四个 PCI 扩展槽或内插连接器。与图 1 中的客户端 108-112 的通信链路可以通过调制解调器 218 和网络适配器 220 来提供，其中调制解调器 218 和网络适配器 220 通过内插连接器连接到 PCI 本地总线 216。

另外的 PCI 总线桥 222 和 214 为另外的 PCI 本地总线 226 和 228 提供接口，由此可以支持另外的调制解调器或网络适配器。以这种方式，数据处理系统 200 允许连接到多个网络计算机。存储器映射图形适配器 230 和硬盘 232 也可以如图所示直接或间接地连接到 I/O 总线 212。

本领域的普通技术人员应当理解，图 2 所示的硬件可以变化。例如，作为对所示硬件的补充或替代，也可以使用其它外围设备如光盘驱动器等。所示例子不旨在暗含对本发明的架构限制。

图 2 所示的数据处理系统可以例如是运行高级交互执行(AIX)操作系统或 LINUX 操作系统的 IBM eServer pSeries 系统，其是国际商业机

器公司、阿芒克、纽约的产品。

现在参照图 3，示出了可以实现本发明的数据处理系统的方框图。数据处理系统 300 可以是如图 1 所示的客户端计算机，或者可以是独立计算设备。数据处理系统 300 采用外围组件互连(PCI)本地总线架构。虽然所示例子采用 PCI 总线，但是也可以使用其它总线架构如加速图形端口(AGP)和工业标准架构(ISA)。处理器 302 和主存储器 304 通过 PCI 桥 308 连接到 PCI 本地总线 306。PCI 桥 308 还可以包括用于处理器 302 的集成存储器控制器和高速缓冲存储器。另外的与 PCI 本地总线 306 的连接可以通过直接组件互连或通过内插板来进行。在所示例子中，局域网(LAN)适配器 310、SCSI 主机总线适配器 312、以及扩展总线接口 314 通过直接组件互连而连接到 PCI 本地总线 306。相反，音频适配器 316、图形适配器 318 和音频/视频适配器 319 通过插入到扩展槽中的内插板而连接到 PCI 本地总线 306。扩展总线接口 314 为键盘和鼠标适配器 320、调制解调器 322 和另外的存储器 324 提供连接。小型计算机系统接口(SCSI)主机总线适配器 312 为硬盘驱动器 326、磁带驱动器 328 和 CD-ROM 驱动器 330 提供连接。典型的 PCI 本地总线实现将支持三个或四个 PCI 扩展槽或内插连接器。

操作系统运行在处理器 302 上，并且用来协调图 3 的数据处理系统 300 内的各个组件，以及提供对其的控制。操作系统可以是可购得的操作系统，例如可从微软公司获得的 Windows XP。面向对象的编程系统如 Java 可以结合操作系统运行，并且提供从在数据处理系统 300 上执行的 Java 程序或应用程序到操作系统的调用。“Java”是太阳微系统公司的商标。操作系统、面向对象的编程系统以及应用程序或程序的指令位于存储设备如硬盘驱动器 326 上，并且可以被装载到主存储器 304 中，以便由处理器 302 执行。

本领域的普通技术人员应当理解，图 3 中的硬件可以根据实现而变化。作为图 3 所示的硬件的补充或替代，可以使用其它内部硬件或外围设备如快闪只读存储器(ROM)、等效非易失性存储器或光盘驱动器等。另外，本发明的处理可被应用于多处理器数据处理系统。

作为另一个例子，数据处理系统 300 可以是被配置成是可引导的而不依赖于某种网络通信接口的独立系统。作为另一个例子，数据处理系统 300 可以是个人数字助理(PDA)设备，其配置有 ROM 和/或快闪 ROM，以便提供非易失性存储器来存储操作系统文件和/或用户生成的数据。

图 3 所示的例子和上述例子不旨在暗含架构限制。例如，除了采取 PDA 的形式之外，数据处理系统 300 也可以是笔记本计算机或手持计算机。数据处理系统 300 也可以是信息站(kiosk)或万维网设备(web appliance)。

如上所述，本发明提供了一种用于将多个安全组表示为单个数据对象的系统和方法。该单个数据对象这里被称作“复合组”数据对象或者 C 组对象。C 组对象被创建为包括组集值和掩码值的数据对象。组集值表示多个组，并且掩码值表示对于相关资源具有特定重要性的组集的子集。

例如，在分布式数据处理环境中，可能存在数百个用户/资源组，其全都由组集值表示。例如，企业可以被划分成区域地点、部门、工作组等。每个区域地点可以具有其自己的超组，每个区域地点的每个部门可以具有其自己的子组，每个区域地点的每个部门内的每个工作组可以具有其自己的子子组，等等。这些组中的每一个可以由单个组集值表示。可选地，可以使用少量的组集值来标识这些组的不同部分。

掩码值用来掩蔽(mask out)对于确定请求者是否被授权访问相关资源而不是必要的组标识符的位。也就是，例如，组标识符可以包括区域标识符、部门标识符、以及工作组标识符。如果资源要可用于特定区域机构(reginal office)的所有用户/资源，则该资源的掩码可以掩蔽与部门标识符和工作组标识符相关联的所有位。也就是，该掩码将允许区域标识符的全部或至少一些位通过，同时清除与部门标识符和工作组标识符相关联的位。

作为具体示例，假定组标识符是 1010 0011 1001。上述掩码值可以采取 1111 0000 0000 的形式。该掩码值指示对相关资源的访问不依赖于

部门或工作组，而是基于用户/资源是否隶属于特定区域机构。可以将掩码值施加到组标识符，以仅仅获得对于授权处理具有重要性的那些位。也就是，可以将掩码值与组标识符进行按位求与，以获得与请求者即提交了访问请求的用户/资源或处理相关联的掩蔽后的组标识符。在上面示例中，对掩码值与组标识符进行按位求与将产生 1010 0000 0000 的掩蔽后的组标识符。

比较所得到的掩蔽后的组标识符和与资源相关联的 C 组对象中的组集值。例如，该比较可以涉及以类似于上面关于请求者的组标识符讨论的方式用相关的掩码值掩蔽组集值，以获得掩蔽后的组集值。例如，假定组集值是 1010 1001 1000。通过将掩码值施加到组集值，即对掩码值和组集值进行按位求与，产生下面的掩蔽后的组集值：1010 0000 0000。

然后，进行掩蔽后的组标识符与掩蔽后的组集值的比较，以确定它们是否匹配。如果它们匹配，则这意味着请求者是由组集值表示的组的一部分。结果，由于 C 组对象标识被授权访问资源的那些用户/资源组，并且请求者的组标识符是由 C 组对象表示的组中的一个或多个组的一部分，因此准予对资源的访问。

图 4 是根据本发明实施例的复合组数据对象的示例图。如图 4 所示，复合组数据对象或 C 组对象 400 包括组集值 410 和掩码值 420。组集值 410 表示实现本发明的数据处理系统的多个用户/资源组。在相同数据处理系统内的多个不同 C 组对象 400 中可以利用相同的组集值 410。

掩码值 420 提供了这样的机制，其用于标识必须由请求者的组标识符匹配以便成功地执行认证处理的组集值 410 的一部分。也就是，掩码值 420 提供了针对特定目的的 C 组对象 400 的可定制性。例如，两个不同的资源可以具有这样的 C 组对象，其具有相同的组集值 410，但是具有不同的掩码值 420。可以使用一个掩码值来指定仅仅管理员级用户能够访问相关资源，同时可以使用其它掩码值来指定与特定部门相关联的所有用户可以被给予对相关资源的访问。

如前所述，一旦针对特定资源或资源组创建了 C 组对象 400，则由计算设备如服务器或独立计算机使用该 C 组对象 400，以执行认证处理。该认证处理确定对访问特定资源的请求者是否与被准予访问特定资源的组相关联。

图 5 是示出根据本发明示例性实施例的数据流的示例图，其用于使用 C 组对象来授权对相关资源的访问。图 5 所示的特定示例性操作用于分布式数据处理环境。应当理解，通过独立计算设备，关于图 5 所述的处理完全可以在相同的计算设备内执行，而不脱离本发明的精神和范围。

如图 5 所示，客户端设备 510 的用户/资源或处理可以将访问请求传送到服务器 520。访问请求将包括被请求访问的资源的标识符、以及请求者即在客户端设备 510 中生成了访问请求的用户/资源或处理的标识符。该请求者标识符被称作组标识符，这是因为它在分布式数据处理系统中标识用户/资源或处理所属的组。

一旦从客户端设备 510 接收到访问请求，服务器 520 就从存储设备 530 中检索在访问请求中指定的资源的复合组数据对象。复合组数据对象或 C 组对象包括组集值和掩码值。例如，通过对掩码值与组标识符和组集值进行按位求与，将掩码值施加到来自访问请求的组标识符和组集值。其结果是掩蔽后的组标识符和掩蔽后的组集值。然后，比较掩蔽后的组标识符和掩蔽后的组集值，以确定是否存在匹配。如果是，则准予对资源的访问。否则，如果不存在匹配，则拒绝访问。

如前所述，组集值表示多个组。可以使用掩码值来从该多个组中选择可以被提供对特定资源的访问的组子集。掩码值和组集值可以针对多个不同的组架构而实现，其中这些组架构例如包括分级组架构、组类别成员关系类型架构、或者分级和组类别成员关系类型架构的混合。在图 6 中提供了这些不同的架构如何由本发明的组集值和掩码值支持的例子。

图 6 是可以与本发明的实施例一起使用的组集值和各种掩码值的示例图。如图 6 所示，可以在复合组数据对象中提供组集值 600。如下所

述，该组集值 600 可以基于由实现本发明的分布式数据处理系统使用的组架构的类型而表示不同的含义。另外，如下所述，掩码值可以根据数据处理系统中的组架构而以多种不同方式组织。在所示特定例子中，在每个示例架构中将使用相同的组集值 600，但是使用不同的掩码值，以便说明基于数据处理系统的组架构解释组集值的区别。

如图 6 所示，基本上存在三个不同的实现本发明的组架构：分级、组类别成员关系(或者被简称作“类别”)、以及混合式组架构。下面描述在这些架构的每一个中本发明的实现。

在分级组成员关系的情况下，组集值表示由复合组数据对象表示的“顶级”分级组。掩码值阐明了请求者必须与其相关联以便获得对资源的访问的特定分级组。该掩码值组织可以以“<分级结构>/全部”表示，其中“<分级结构>”是宽度为<n>位的字段内的特定位模式。“全部”是具有宽度<大小>－<n>位的“0”位串，其中“<大小>”是以位为单位的组集值的宽度。在所示例子中，<大小>是 12 位，<n>是 8 位，并且“全部”串的宽度为 4 位。

在图 6 所示的特定例子中，分级掩码被分解成表示特定数据处理系统的分级结构的各个级别的位串。例如，该分级结构的高级别由标识区域机构的“物理地点”610 表示。“物理地点”610 的子集是“部门”620，并且“部门”的子集是“工作组”630。这样，通过图 6 所示的分级掩码值，可以将物理地点、部门和工作组的各种组合指定为允许访问特定资源。

在所示例子中，掩码值是 1101 1100 0000。物理地点 610 和部门 620 表示掩码值的“<分级结构>”，并且工作组 630 是“全部”0 位串。这样，由 610 和 620 中的掩码值指定的请求者的组标识符的特定分级位必须匹配组集值 600。

作为例子，假定请求者的组标识符是 1011 1011 1111。图 6 中的分级掩码值指示了请求者必须与由位串 610 表示的一个或多个物理地点相关联，并且必须与由位串 620 表示的一个或多个部门相关联。在该特定例子中，请求者与其相关联的特定工作组对于确定请求是否被授权是无关紧要的。

当将请求者的组标识符值与掩码值进行求与时，其结果是 1001 1000 0000。当将分级掩码值与组集值进行求与时，其结果是1001 1000 0000，因此存在匹配。这样，请求者将被提供对资源的访问。另一方面，如果请求者的组标识符是 1101 1011 1111，则施加掩码的结果将是 1101 1000 0000，并且将不存在匹配。从而，请求者将不被提供对资源的访问。

在组类别成员关系架构或者简称的“类别”架构的情况下，组集值可以表示“低级别”成员关系，其中掩码值表示请求者必须与其相关联以便获得对资源的访问的一个或多个类别。这种类型的掩码值可以以“全部/<类别>”表示，其中“全部”同样是 0 位串。在这种情况下，“全部”的宽度为<n>位，其中<n>是用来选择组集值的分级部分的掩码值的宽度。“<类别>”部分是具有宽度<大小>－<n>位的字段内的特定位模式，其中“<大小>”是以位为单位的组集值的宽度。

在图 6 所示的特定例子中，类别掩码被分解成表示特定物理地点 640、部门 650 和工作组 660 的位串。在所示例子中，<大小>将同样为 12 位，<n>将是 8 位，因为这两个部分 640 和 650 用来表示特定分级结构，并且<类别>将是 4 位。如图所示，分级结构位在类别掩码中已被清除，使得它们对于确定对相关资源的访问请求是否被授权是无关紧要的。只有请求者与其相关联的特定工作组对于该授权处理是重要的，而与特定的物理地点或部门无关，即只有请求者的类别是重要的。

在所示例子中，被允许访问特定资源的请求者仅仅是与由工作组部分 0101 表示的工作组相关联的那些请求者。任何其它工作组如 1101、1000、1111 等将不能够访问特定资源。然而，例如，如果类别掩码值被修改为 0000 0000 1101，则其组标识符的工作组部分具有 01x1 形式的任何工作组将能够访问相关资源，其中 x 是 0 或 1。类似地，如果类别掩码值被修改为 0000 0000 0101，则其组标识符的工作组部分具有 x1x1 形式的任何工作组将能够访问相关资源，而与工作组的特定物理地点或部门无关，其中 x 是 0 或 1。

在混合式组架构的情况下，组集值被划分为多个位字段。在所示例

子中，组集值被划分成表示特定数据库的字段 670、表示特定部门的字段 680、以及表示特定任务的字段 690。例如，每个字段具有其自己的宽度<i>、<j>和<k>。在所示例子中，<i>、<j>和<k>中的每一个的宽度为 4 位，然而，在其它实现中，这些宽度中的每一个可以相互不同。这些字段相互之间的依赖性或独立性是实现特定的，然而，依赖性或独立性的任何措施可以由该混合式架构表示。

例如，如图 6 所示，混合掩码值具有值 1101 0000 1111。该掩码值意味着对相关资源的访问依赖于数据库和正被执行的特定任务。请求者的特定部门对于对资源的访问的授权是不重要的。结果，其组标识符具有以下形式 10x1 xxxx 0101 的任何请求者将被准予对资源的访问，其中 x 是 0 或 1。

这样，本发明允许由具有组集值和掩码值的单个复合组数据对象表示多个用户/资源/处理组。授权请求的处理涉及将复合组数据对象的掩码值施加到请求者的组标识符和复合组数据对象的组集值，以确定是否存在匹配。如果是，则向请求者准予对访问资源的授权。如果不存在匹配，则拒绝访问。由于施加掩码和确定匹配的处理是认证访问请求所需的唯一处理，因此特定数据处理系统的组架构的大小不会显著影响认证处理的性能。处理更复杂的组架构只需在组集值和掩码值的部分中提供附加位。

另外，本发明在处理各种组架构上提供了很大灵活性。例如，本发明可以用来定义诸如“会计”、“营销”、“研究”的数据库子组，并且定义诸如“备份”、“创建”等的数据库任务。然后，对于这些不同的子组和数据库任务，可以以混合且匹配的方式定义组集值。

例如，备份数据库的授权可以要求允许访问“备份”工具的组或复合组(其具有请求者在“备份”组中具有成员关系的请求者)、以及允许访问数据的组或复合组(其具有这样的要求，即请求者在与数据相关联的某组中具有成员关系)。在被表达为组和复合组的情况下，用户将被要求在传统组“备份”中、或者在具有“全部/备份”作为其值(也就是，除了选择“备份”功能性的那些位之外，起始全都为零的掩码值)的复合组中具

有成员关系。另外，用户还将被要求在允许访问特定数据的组或复合组中具有成员关系。例如，由组“数据库/总部/会计”拥有的文件将要求具有该特定值的传统组、允许访问所有“数据库”(例如，数据库/全部)文件、所有“总部”文件(例如，全部/总部/全部)、所有“会计”文件(例如，全部/全部/会计)或者某其它组合如数据库/全部/会计的复合组。

图 7 是概述本发明一个实施例的示例性操作的流程图。应当理解，流程图中的每个块、以及流程图中的多个块的组合可以通过计算机程序指令实现。这些计算机程序指令可以被提供给处理器或其它可编程数据处理设备，以产生一种机器，使得在处理器或其它可编程数据处理设备上执行的指令创建用于实现在一个或多个流程图块中指定的功能的装置。这些计算机程序指令还可以被存储在计算机可读存储器或存储介质中，其可以引导处理器和其它可编程数据处理设备以特定方式工作，使得存储在计算机可读存储器或存储介质中的指令产生包括实现在一个或多个流程图块中指定的功能的指令装置的产品。

从而，流程图中的块支持用于执行指定功能的装置的组合、用于执行指定功能的装置的组合、以及用于执行指定功能的程序指令装置。还应当理解，流程图中的每个块、以及流程图中的多个块的组合可以通过执行指定功能或步骤的基于专用硬件的计算机系统实现，或者通过专用硬件和计算机指令的组合实现。

如图 7 所示，该操作通过接收具有与请求者相关联的组标识符的访问请求并且识别期望访问的资源(步骤 710)。然后，检索与资源相关联的复合组对象(步骤 720)。如前所述，该复合组对象包括组集值和掩码值。

然后，将复合组掩码值施加到请求者的组标识符，即在访问请求中接收的组标识符(步骤 730)。如前所述，例如，将掩码值施加到组标识符可以包括对掩码值与组标识符进行按位求与，以获得掩蔽后的请求者的组标识符。

还将复合组掩码值施加到复合组中的组集值(步骤 740)。同样，这可以涉及对复合组掩码值与组集值进行按位求与，以获得掩蔽后的组集

值。应当注意，由于步骤 740 的结果具有不变值，因此可以在创建复合组数据对象时执行该步骤。

比较所得到的掩蔽后的组集值和掩蔽后的请求者的组标识符(步骤 750)，并且确定它们是否匹配(步骤 760)。如果否，则拒绝对资源的访问(步骤 770)。如果它们匹配，则准予访问(步骤 780)。然后，授权处理结束。

这样，本发明提供了一种用于将多个用户/资源组表示为单个组数据对象的系统和方法。通过本发明，可以使用相同的组集值来表示多个不同组。可以向资源提供不同的掩码值，以便识别组集值中的哪些组被授权访问相关资源。结果，可以向多个资源提供复合组对象，其全都具有相同的组集值，但是可以针对它们的特定目的而具有不同的掩码值。

通过本发明，授权对给定资源的访问所需的处理量保持相同，而与组数无关。可以通过增加组集值和掩码值中的位数来增加另外的组。然而，授权处理将总是由这样的两步骤处理组成，即对所接收的组标识符进行掩蔽，并且将掩蔽后的组标识符与资源的复合组对象的组集值相比较。换句话说，由计算系统维护的“组”结构的大小不会显著地影响本发明的授权处理的性能。

如上所述，本发明尤其有用于实现分布式计算系统资源的访问控制列表。另外，本发明可以与其它访问控制机制一起使用，而不脱离本发明的精神和范围。简而言之，访问相关实体所需的成员关系可以由组集值和掩码值表示的任何控制机制可以利用本发明。

值得注意的是，虽然本发明是在全功能数据处理系统的上下文中描述的，但是本领域的普通技术人员应当理解，本发明的处理能够以包含指令的计算机可读介质的形式和各种形式分发，并且本发明都同样适用，而与实际用来执行分发的信号承载介质的特定类型无关。计算机可读介质的例子包括可记录型介质，例如软盘、硬盘驱动器、RAM、CD-ROM、DVD-ROM，以及传输型介质，例如数字和模拟通信链路、使用诸如射频和光波传输的传输形式的有线或无线通信链路。计算机可读介质可以采取编码格式的形式，其中编码格式为了在特定数据处理系统

中实际使用而被解码。

本发明的描述是为了示例说明的目的而提供的，而不旨在是彻底无遗漏的，或者局限于所公开的实施例。很多修改和变更对于本领域的普通技术人员将是清楚的。选择和描述该实施例是为了最佳地说明本发明的原理及其实际应用，并且使得本领域的其他普通技术人员能够理解本发明，以便实现适于特定预期用途的具有各种修改的各种实施例。

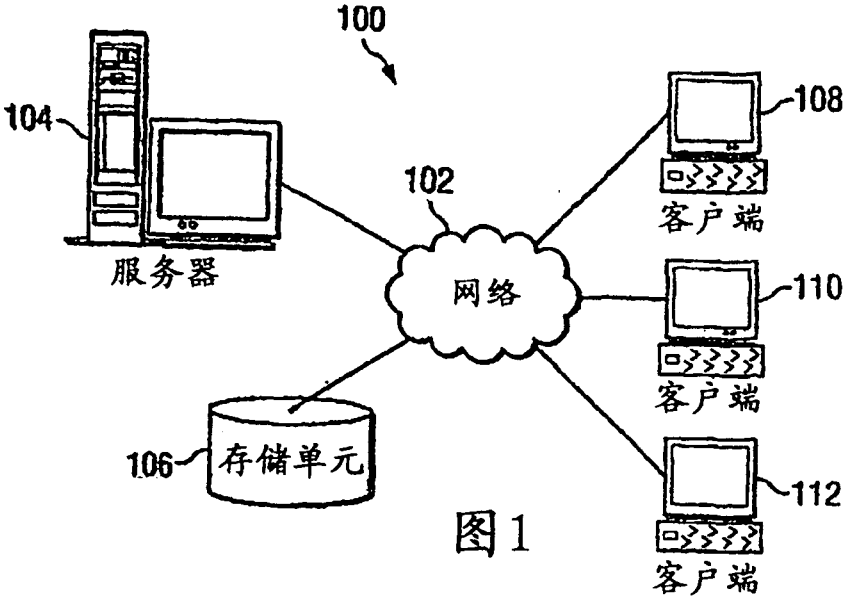

100
104
服务器
102
网络
108
客户端
110
客户端
112
客户端
106
存储单元

图1

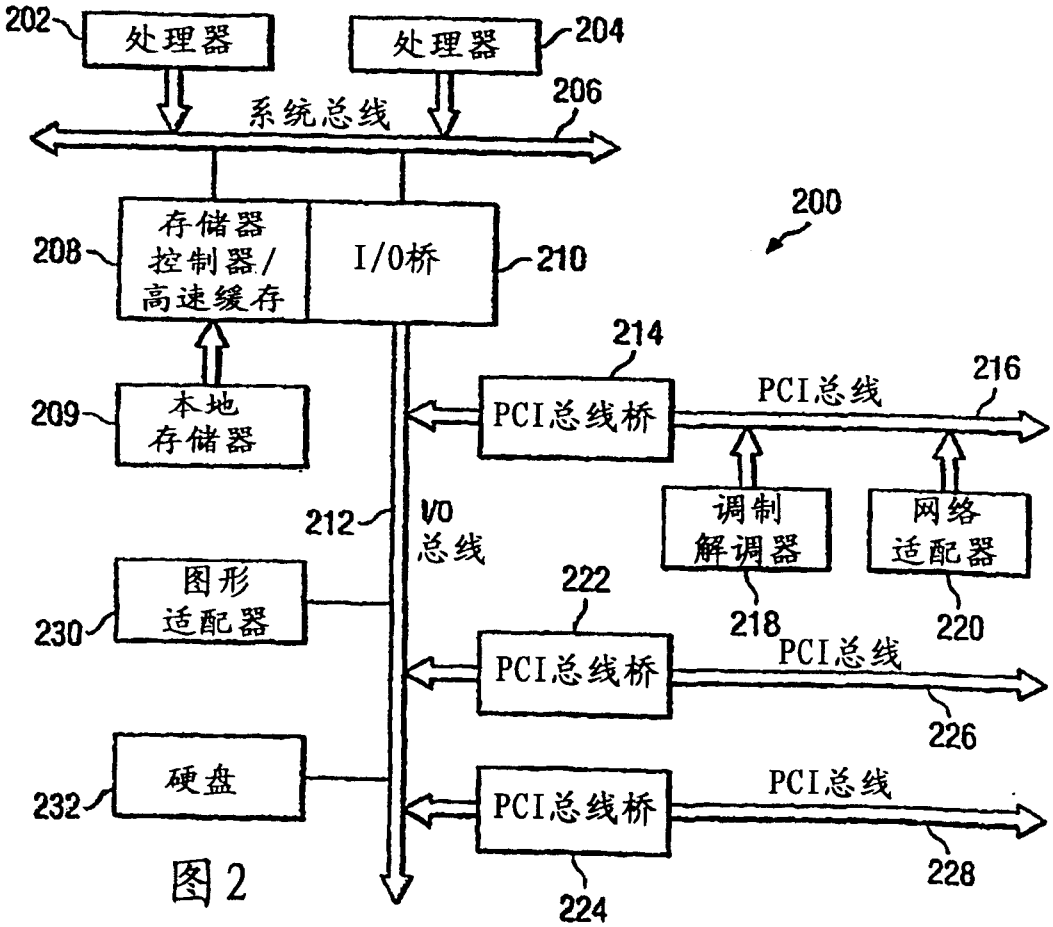

202
处理器
处理器
204
206
系统总线
200
208
存储器
控制器/
高速缓存
I/O桥
210
214
209
本地
存储器
PCI总线桥
PCI总线
216
212
I/O
总线
调制
解调器
网络
适配器
222
图形
适配器
230
218
220
PCI总线桥
PCI总线
226
硬盘
232
PCI总线桥
PCI总线
228
224

图2

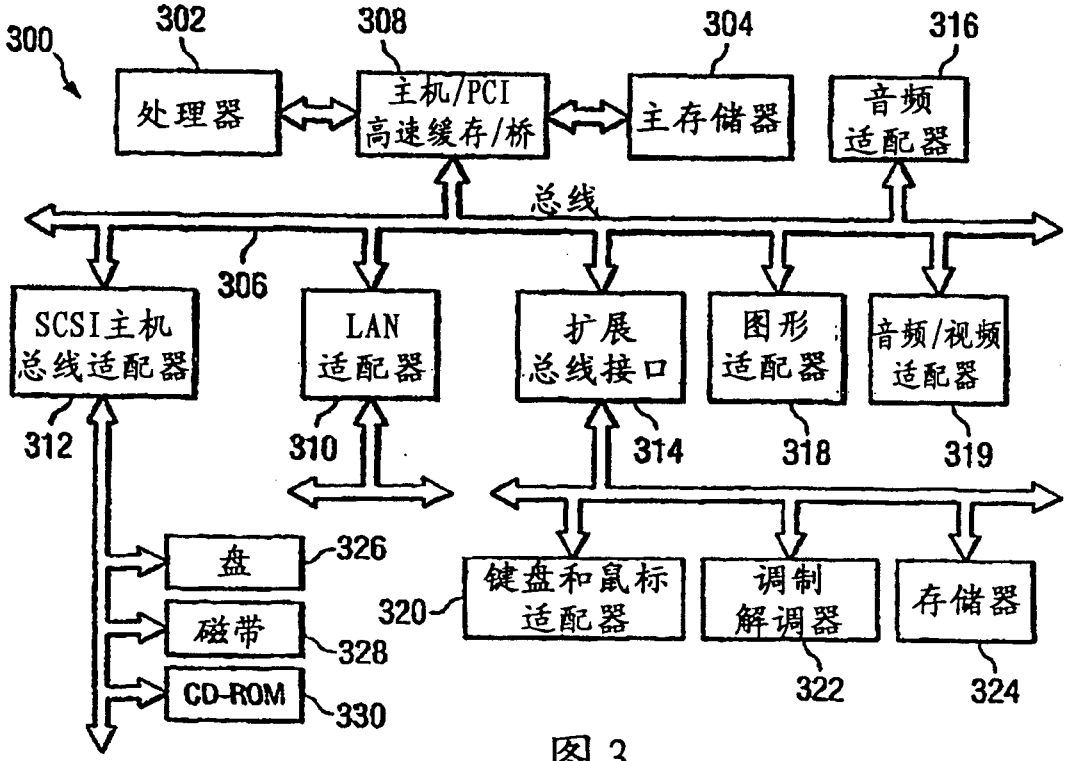

300
302
处理器
308
主机/PCI
高速缓存/桥
304
主存储器
316
音频
适配器
总线
306
SCSI主机
总线适配器
312
LAN
适配器
310
扩展
总线接口
314
图形
适配器
318
音频/视频
适配器
319
盘
326
磁带
328
CD-ROM
330
320
键盘和鼠标
适配器
调制
解调器
322
存储器
324

图 3

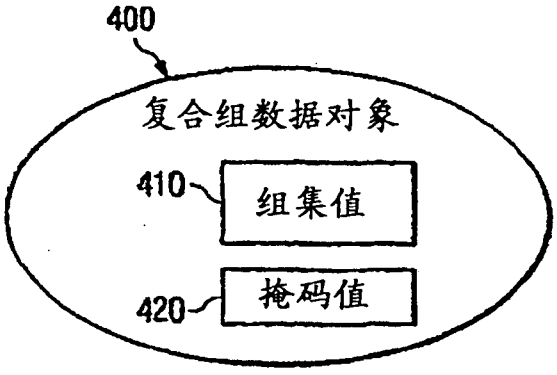

400
复合组数据对象
410
组集值
420
掩码值

图 4

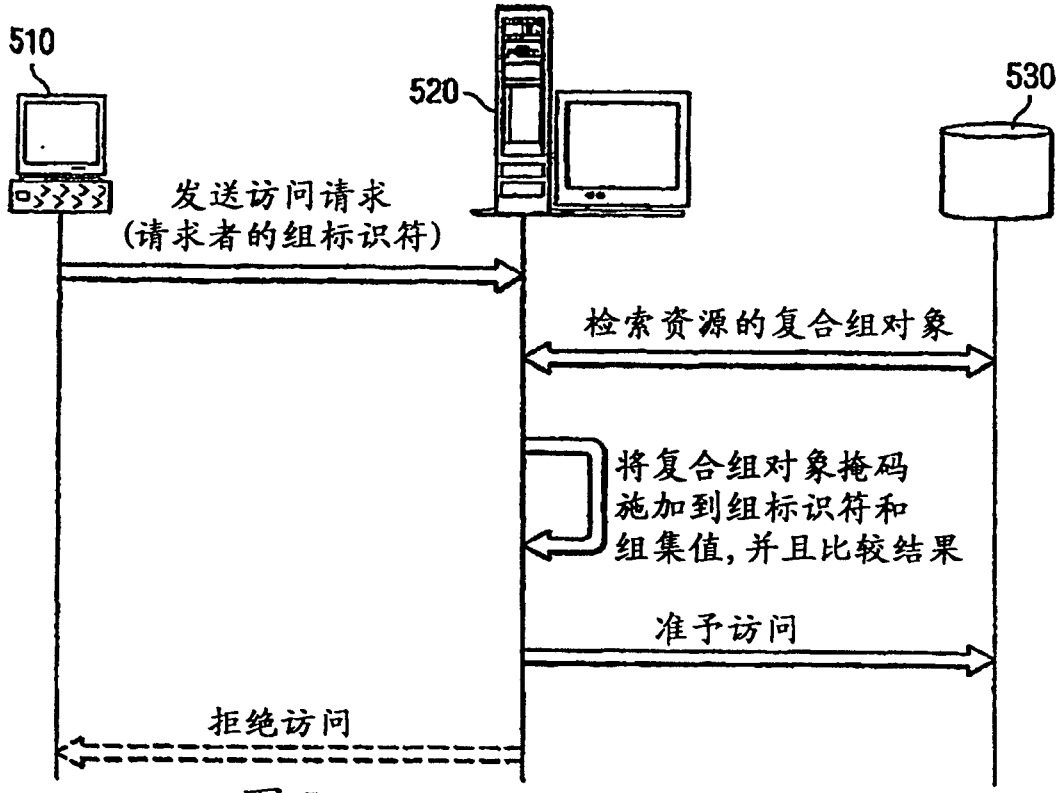

510
520
530
发送访问请求
(请求者的组标识符)
检索资源的复合组对象
将复合组对象掩码
施加到组标识符和
组集值,并且比较结果
准予访问
拒绝访问

图5

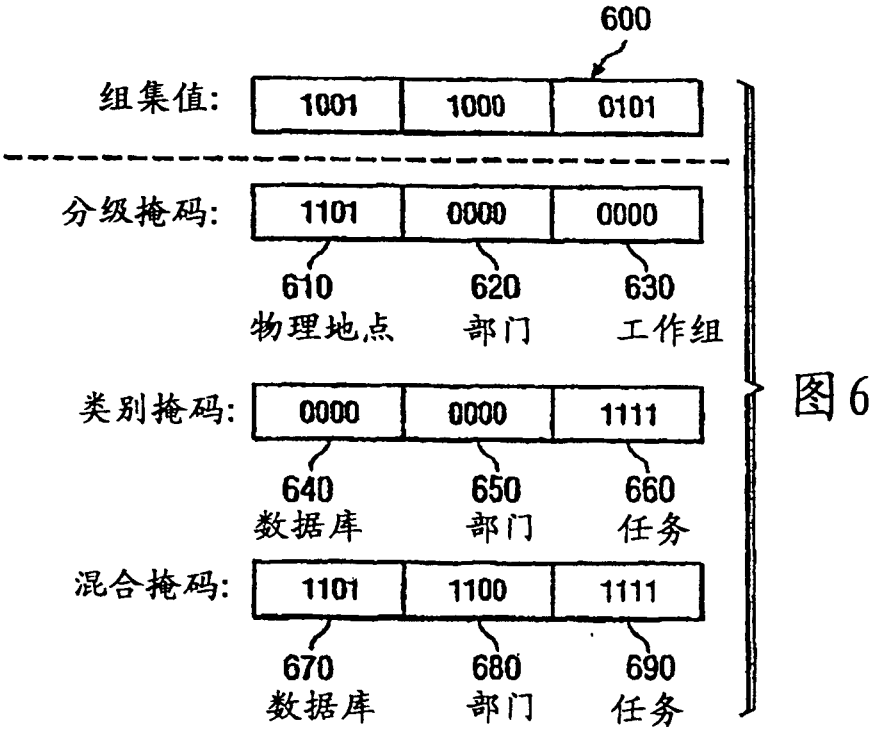

600
组集值:
1001
1000
0101
分级掩码:
1101
0000
0000
610
物理地点
620
部门
630
工作组
类别掩码:
0000
0000
1111
640
数据库
650
部门
660
任务
混合掩码:
1101
1100
1111
670
数据库
680
部门
690
任务

图6

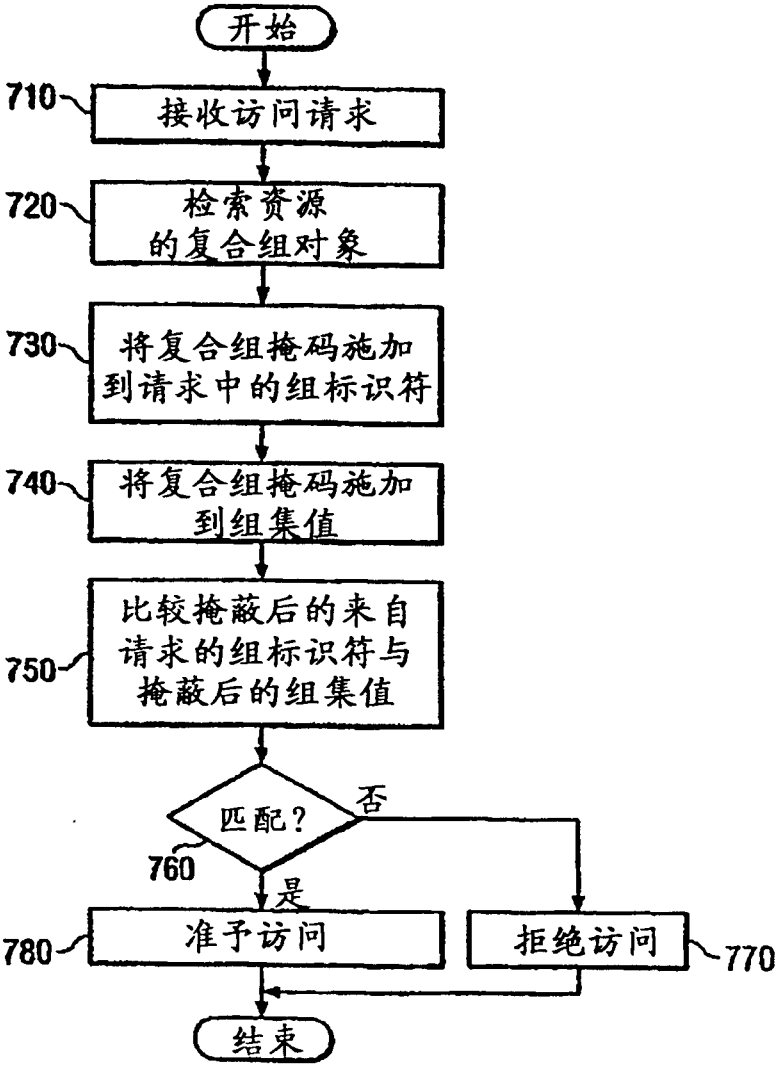

开始
710
接收访问请求
720
检索资源
的复合组对象
730
将复合组掩码施加
到请求中的组标识符
740
将复合组掩码施加
到组集值
750
比较掩蔽后的来自
请求的组标识符与
掩蔽后的组集值
匹配?
760
否
是
780
准予访问
拒绝访问
770
结束

图7