[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/00

# [12] 发明专利申请公开说明书

[21] 申请号 96113317.1

[43]公开日 1997 年 5 月 14 日

[11] 公开号 CN 1149797A

[22]申请日 96.8.17

[30]优先权

[32]95.8.18 [33]US[31]516,671

[71]申请人 太阳微系统有限公司

地址 美国加利福尼亚州

[72]发明人 D·M·内塞特

T·D·托克

[74]专利代理机构 中国专利代理(香港)有限公司

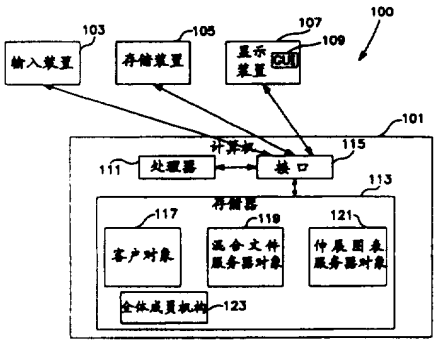
代理人 邹光新 傅 康

权利要求书 7 页 说明书 10 页 附图页数 3 页

[54]发明名称 在分布系统中用于对系统资源可靠控制存取的方法和系统

[57]摘要

一种用来在分布计算机系统对资源可靠地控制存取的改进方法和系统。本发明的一个实施例对目标对象存储和赋置组标记，然后使用全体成员核对来确定对目标对象请求存取的客户对象是否是具有对目标对象存取权的组织的成员。本发明的第二个实施例存储和赋值目标对象基准的组标记，然后把目标对象基准传送到系统中的客户对象。由于目标对象基准包括组标记登记,因此第一客户对象能够确定系统中其它客户是被识别组的成员。



# 权 利 要 求 书

1.一在分布计算机系统中用于对系统资源控制存取的计算机系统实施方法，该方法包括下述步骤：

把来自客户对象的请求送给伸展图表服务器，以对伸展图表对象赋以组标志符；

在伸展图表服务器控制下，

获得伸展图表对象；

存储具有伸展图表对象的组标志符；

产生不会伪造的检查和；

存储具有伸展图表对象的不会伪造的检查和；

把不会遗忘的检查和送到顾客对象；

在客户对象的控制下，

把请求送到混合文件服务器，以打印混合文件；

在混合文件服务器的控制下，

把请求送到伸展图表服务器以请求伸展图表服务器从伸展图表对象返送数据；

在伸展图表服务器控制下，

基于组标志符的分析允许或拒绝对伸展图表对象的存取。

2.一种在分布计算机系统中便于对系统资源存取控制的计算机系统实施方法，该分布计算机系统包括客户对象、第一服务器对象、目标对象和第二服务器对象，这些对象的每一个属于一个或多个存在于计算机系统的对象指定组，该方法包括以下步骤：

在第一服务器对象的控制下，

存储具有目标对象的组标志符，该组标志符用对目标对象的存取特权表示系统中对象的组；

在第二服务器对象控制下，

获得贮存器对象；

把请求送给请求对目标对象存取的第一服务器对象，该请求包括识别以第

二服务器对象名义操作的委托人的委托人标志符；和

在第一服务器控制下，

检验第二服务器许可使用存储于目标对象中的组标志符和包括在来自第二服务器请求中的委托人标志符来存取目标对象。

3.根据权利要求2所述的方法， 其特征在于获取贮存器对象的步骤进一步包括：

在第一服务器对象的控制下，

把目标对象基准传送给客户对象，该目标对象基准指出计算机系统中的目标对象位置；

在客户对象的控制下，

安置以属于客户对象组的成员名义操作的第二服务器；

把请求送给被安置的第二服务器，请求第二服务器获得参考该目标对象的贮存器对象，从客户对象到第二服务器对象的请求包括目标对象基准，该请求还包括识别客户对象属于该组的组标志符；

在第二服务器的控制下，

获得贮存器对象；和

在贮存器对象中存储目标对象基准和组标志符。

4.根据权利要求2所述的方法， 其特征在于把来自第二服务器的请求送给第一服务器的步骤包括：

在客户对象的控制下，

把请求送给第二服务器以使用贮存器对象，该请求包括贮存器的基准和客户对象的委托人的标志符；和

在第二服务器控制下，

响应来自客户对象的请求，把请求送入第一服务器以存取目标对象，该请求包括目标对象的基准和代表第二服务器操作的委托人的标志符。

5.根据权利要求4的方法，进一步包括以下步骤：

在第一服务器控制下，

使用从第二服务器送到第一服务器的委托人识别来鉴别第二服务器。

6.根据权利要求5所述的方法，进一步包括以下步骤：

当第二服务器被授权和被确定是具有对目标对象的存取权的组的成员时，

确定第二服务器是否授权以被请求的方式存取目标对象，

从第一服务器基准检索不会伪造的数字；

把被检索的不会伪造数字与存有目标对象的不会伪造数字相比较；和

当这些不会伪造数字相一致时，在第二服务器的存取权控制下允许服务器存取目标对象。

7.根据权利要求2所述的方法， 其特征在于检验第二服务器许可存取目标对象的步骤进一步包括：

在第一服务器控制下，

从目标对象中检索组标志符；

把被检索组标志符和委托人标志符同确定委托人是否是具有对目标对象的存取权的组成员的请求一起送到全体成员机构；和

当第二服务器被确定是以委托人名义操作时，允许第二服务器存取目标对象，这里所说的委托人是具有对目标对象的存取权的组的成员。

8.根据权利要求2所述的方法，进一步包括：

把来自顾客对象的请求送到第一服务器对象，该请求表示第一服务器对象应建立目标对象；和

在第一服务器对象的控制下，

建立目标对象；和

存储组成员有涉及目标对象的存取权的标记。

9.在分布计算机系统中便于对系统资源存取控制的计算机系统，该分布计算机系统包括客户对象，第一服务器对象、目标对象和第二服务器对象，这些对象中的每一个属于一个或多个存在于计算机系统中对象的指定组，该系统包括：

形成的第一服务器对象，以

存储具有目标对象的组标志符，该组标志符用对目标对象的存取特权表示系统中对象的组；

形成的第二服务器对象，以

获取贮存器对象；

把请求送到第一服务器对象以对目标对象请求存取，该请求包括识别以第二服务器名义操作的委托人的委托人标志符；和

形成第一服务器，以

检验第二服务器允许靠使用存储于目标对象中的组标志符和含有来自第二服务器请求中的委托人标志符去存取目标对象。

10.根据权利要求9所述的系统，其特征在于获取贮存器对象进一步包括一个系统，其中：

形成第一服务器对象，

把目标对象基准送到客户对象，该目标对象基准指示计算机系统中目标对象的位置；

形成客户对象，

安置以属于客户对象组成员名义操作的第二服务器；

把请求送到被安置的第二服务器，请求第二服务器获得参考目标对象的贮存器对象，从客户对象到第二服务器对象的请求包括目标对象基准，该请求还包括识别客户对象属于该组的组标志符；和

形成第二服务器，

获得取贮存器对象；和

在贮存器对象中存储目标对象基准和组标志符。

11.根据权利要求9所述的系统，其特征在于把来自第二服务器的请求送到第一服务器进一步包括一个系统，其中：

形成客户对象，

把请求送到第二服务器以使用贮存器对象，该请求包括贮存器对象的基准和客户对象的委托人的标志符；和

形成第二服务器，

响应来自客户对象的请求，把请求送入第一服务器以存取目标对象，该请求包括目标对象的基准和以第二服务器名义操作的委托人的标志符。

12.根据权利要求11所述系统进一步包括：

形成第一服务器，

使用从第二服务器送到第一服务器的委托人的识别鉴别第二服务器。

13.根据权利要求12所述的系统进一步包括形成的机构：

当第二服务器被鉴别和被确定是具有对目标对象的存取权的组的成员时，确定第二服务器是否授权以被请求的方式存取目标对象，

从第一服务器基准中检索不会伪造的数字；

把被检索的不会伪造数字与存有目标对象的不会伪造数字相比较；和

当这些不会伪造数字相一致时，在第二服务器存取权的控制下允许第二服务器存取目标对象。

14.根据权利要求9所述的系统，其特征在于检验第二服务器允许存取目标对象进一步包括一个系统，其中：

形成第一服务器，

从目标对象中检索组标志符；

把被检索组标志符和委托人标志符与确定委托人是否是具有目标对象的存取权的组成员的请求一起送到全体成员机构；和

当第二服务器被确定是以委托人名义操作时，允许第二服务器存取目标对象，这里所说的委托人是具有对目标对象的存取权的组的成员。

15.根据权利要求9所述的系统进一步包括形成的机构：

把来自客户的请求送到第一服务器对象，该请求包括第一服务器应该建立目标对象；和

形成第一服务器对象，以

建立目标对象；和

存储组成员有涉及目标对象的存取权的标记。

16.在分布计算机系统中便于对系统资源存取控制的计算机程序， 该分布计算机系统包括客户对象、第一服务器对象、目标对象和第二服务器对象，这些对象中的每一个属于一个或多个存在于计算机系统中对象的指定组，该程序包括：

形成的第一服务器对象的程序指令，以

存储具有目标对象的组标志符，该组标志符用对目标对象的存取特权表示系统中对象的组；

形成的第二服务器对象的程序指令，以

获取贮存器对象；

把请求送到第一服务器对象以对目标对象请求存取，该请求包括识别以第二服务器名义操作的委托人的委托人标志符；和

形成的第一服务器的程序指令，以

检验第二服务器允许靠使用存储于目标对象中的组标志符和含有来自第二服务器请求中的委托人标志符去存取目标对象。

所说的程序指令存储在有形媒体上。

17.根据权利要求 16 所述的程序， 其特征在于获取贮存器对象进一步包括:

形成的第一服务器的程序指令，以

把目标对象基准送到客户对象，该目标对象基准指示计算机系统中目标对象的位置;

形成的客户对象的程序指令，以

安置以属于该组成员名义操作的第二服务器；和

把请求送到被安置的第二服务器，以请求第二服务器获得参考目标对象的贮存器对象，从客户对象到第二服务器对象的请求包括目标对象基准，该请求还包括识别客户对象属于该组的组标志符；和

形成的第二服务器的程序指令，以

获取贮存器对象；和

在贮存器对象中存储目标对象基准和组标志符。

18.根据权利要求16所述的程序， 其特征在于把来自第二服务器的请求送到第一服务器进一步包括:

形成的客户对象的程序指令，

把请求送到第二服务器以使用贮存器对象，该请求包括贮存器对象的基准和客户对象的委托人的标志符；和

形成的第二服务器的程序指令，

响应来自客户对象的请求，把请求送到第一服务器以存取目标对象，该请求包括目标对象的基准和以第二服务器名义操作的委托人的标志符。

19.根据权利要求18所述的程序进一步包括:

形成的第一服务器的程序指令，

使用从第二服务器送到第一服务器的委托人的识别鉴别第二服务器。

20.根据权利要求19所述的程序进一步包括形成的程序指令:

当第二服务器被鉴别和被确定是具有对目标对象的存取权的组的成员时，确定第二服务器是否授权以被请求的方式存取目标对象，

从第一服务器基准中检索不会伪造数字；

把被检索的不会伪造数字与存有目标对象的不会伪造数字相比较；和

当这些不会伪造数字相一致时，在第二服务器存取权的控制下允许第二服务器存取目标对象。

21.根据权利要求16所述的程序， 其特征在于检验第二服务器允许存取目标对象进一步包括：

形成的第一服务器的程序指令，

从目标对象中检索组标志符；

把被检索组标志符和委托人标志符与确定委托人是否是具有目标对象的存取权的组成员的请求一起送到全体成员机构；和

当第二服务器被确定是以委托人名义操作时，允许第二服务器存取目标对象，这里所说的委托人是具有对目标对象的存取权的组的成员。

22.根据权利要求16所述的程序进一步包括形成的程序指令：

把来自客户的请求送到第一服务器对象，该请求包括第一服务器对象应该建立目标对象；

形成第一服务器对象的程序指令，

建立目标对象；和

存储组成员有涉及目标对象的存取权的标记。

# 说　明　书

## 在分布系统中用于对系统资源可靠控制存取的方法和系统

本发明的方法和系统涉及计算机系统中通常提供的可靠性，特别涉及利用向对象基准或权能赋值的组织识别来控制对系统资源的存取。

在面向对象系统中，对象是包括数据和可以被调用去控制数据的操作的元素。操作(也称作"方法")通过把向对象发送一呼叫而在对象上被调用。每个对象有限定操作的对象类型，该操作可在以那个类型的对象上实行。一个对象类型可继承对别的对象类型限定和实施对象操作。面向对象设计和设计程序技术的进一步说明参见"面向对象软件结构"由Bertrand Mejer, Prentice-Hall在1988年提出(该资料可作为参考文献)。

在客户—服务器计算中，一般有一组计算机，它可以通过连接若干计算机的网络而与另外的计算机相互通信。这些计算机的一些作为对别的计算机服务和功能的提供者。该服务或功能的提供者称为"服务器"，服务或功能的消费者(用户)称为"客户"。客户—服务器模式还概括为这样一种情况，在同一计算机上运行性质不同的程序或进程和通过某些保护机构与另一计算机上运行的不同程序进程相互通信以及作为功能的提供者和消费者。

在基于客户—服务器模式的面向对象的分布系统中，存在向其客户提供面向对象的接口的一些服务器。为了操纵该数据这些服务器根据由对象类型所允许的操作支持由数据和控制数据的相关软件组成的对象。通过对该服务器传送呼叫，服务器可获得对这些对象的存取并可在这些对象上执行呼叫。对服务器来说，这些呼叫是通过与对象相关软件而被执行的。这些呼叫的结果返回到客户。

目前，许多公司已同意统一某些对象定义和接口标准允许相互之间共享这样的对象。一种设计成能够以这种互联伙伴分享对象的方式参与（合作）的系统被称之为"分布对象环境("DOE")，由Sun Microsystems公司提出，注册。

DOE是一种面向对象系统，提供了从客户到DOE对象的遥控存取。服务器申

请实施DOE对象。对于任何给定的DOE对象，DOE服务器可以建立作为DOE对象指示符的对象基准。DOE 对象基准可以在一个机器上或不同机器间的不同进程之间传送，它将仍然指示原来的对象。

当一个位置上的客户应用获得DOE对象基准时，它可以把呼叫（系统调用请求）送到目标DOE对象，然后目标DOE对象可以执行这些呼叫，允许更新内部状态(数据)并允许把某些结果返回呼叫者。作为处理一方法调用的一部分，服务器可自行调用其他对象，建立对象调用链。

与处于用户直接控制之外的机构分享这种对象的出现，引发了许多可靠性问题。例如，允许DOE用户存取散布在大型设备中的对象是我们所期望的，但是最重要的是确保只有被授权用户允许存取对象，所以对象封闭的数据不可利用或不能由未授权用户改变。

作为这种可靠性关系的部分解决，某些服务器对它的对象提供可靠存取，以便只有适当指定的用户可以存取对象。当客户申请对可靠的对象存取时，它必须与含有可靠对象执行程序的服务器建立授权关系。在建立这种联系时，客户申请必须向服务器证实该客户申请是表示哪个用户。例如，客户申请也许表示的是用户Susan。(作为存入客户计算机业务的一部分，表明是Susan 的用户将不得不提供某些类型鉴别信息，例如对客户计算机的密码。）在鉴别关系建立后，服务器被确认以致由给定的关系接到被授权代表给定用户的申请。该服务器将记录这个用户的名字和将这个用户的名字与给定的关系相联系。建立鉴别关系的技术是众所周知的，作为例子请参见"分布系统中的鉴别：理论和原理"，由Butler Lampson, Martin Abadi, Michael Burrows 和Edward Wobber提出，登载在1992年的ACM计算机系统学报10(4)期上。

正常的DOE模式是在遥控对象上客户调用操作。服务器可以请求在被鉴别的关系上提出请求，因而可以确认客户申请正代表被鉴别用户。然后服务器可以执行核查，以观察这个被鉴别用户是的确被授权而进行该操作。

用户要服务器执行某些要求服务器存取某些别的可靠服务器的行动就会出现困难。例如，用户可请求客户申请获得混合文件(例如，含有伸展图表曲线和说明正文的年度销售报告)，在第一服务器上安置混合文件的一部分(例如正文)，而在第二服务器上安置混合文件的一部分(例如曲线)。第一服务器可以鉴别请求的用户和验证用户被授权提出请求。然而，如果第一服务器接着必须

为了某些数据第二服务器以完成用户答复，那么第二服务器就必须鉴别第一服务器和必须确保第一服务器由客户许可存取或有足够的存取许可，以在对象上执行它的请求行为。该问题被称为委托问题。无论该问题什么时候出现，为了允许客户进行工作，顾客委托其对服务器的授权部分是必需的。

由用户对以存取第二服务器的方式在用户的名字中起作用的指定服务器的委托，要求用户依靠许多机器，保留这些机器容易受到可靠性侵害；或者用户必须依靠小型的现有机器，它严格地限制了用户对期望的对象的存取。同样，来自分布在网络上的顾客的存取请求对服务器本身提出了具体的可靠性风险。这样，在分布的和网状的环境中开发用于可靠地委托存取控制权的改进方法和系统将是所期望的。

本发明以一种精致和简单的方式解决在网络环境的分布计算机系统中可靠地处理来自各个服务器的存取请求问题，在下面将作更为全面的介绍。

本发明的实施例提供了在分布计算机系统中对资源可靠控制存取的改进方法和系统。本发明的一个实施例存储和赋值具有目标对象的组标识，然后，使用全体成员验证以确定以用户名义向目标对象请求存取的客户对象是否是该组的成员。这样，本发明就避免了像常见的某些现有系统那样为验证请求对象的存取权所进行的昂贵的加密操作。

本发明的第二个实施例向目标对象基准存储和赋值组标识，然后把目标对象基准传送到系统中的客户对象。由于目标对象基准包括组标识入口，因此第一客户对象能够确定系统中的其它客户是被标识组的成员。这个确定允许第一客户对象把目标对象基准传送到该组的其它成员，而不需要首先与目标对象的服务器联系。这样，本发明就避免了与目标对象的服务器联系的昂贵的业务费用。

下面的详细说明主要是依据计算机数据比特操作的方法和符号表示法进行的。这些方法的说明和表示是现行数据技术领域的普通技术人员所使用的能非常有效地把他的工作的内容传递给本技术领域的其他普通技术人员的方法。

方法在这里通常被想象为导致期望结果的步骤的自相容指令序列。这些步骤需要实际参数的实际操作。通常(尽管不是全部)，这些参数采用能够存储、变换、组合、比较和其它操作的电或磁信号形式。它有时证明是很方便的，这主要是因为共同使用了所涉及的这些信号，如比特、数值、元素、符号、特性、

术语、数字或类似物。这些内容应该是处于记忆之中，然而，所有这一切和相似术语都是与适当的实际参数相关联而且仅仅是适于这些参数的方便的信息识别符。

用于执行本发明操作的有用机器包括普通用途数字计算机或相似装置。该普通用途计算机由存储在计算机中的计算机程序有选择地启动或重新配置。特殊用途计算机也可以执行本发明的操作。总之，这里说明和建议的方法应用不限于特殊的计算机结构。

图1是用于实施本发明优选实施例的计算机系统的方框图；

图2 是说明用于对系统资源可靠控制存取的第一实施例的优选步骤的流程图；

图3 是说明用于对系统资源可靠控制存取的第二实施例的优选步骤的流程图。

本发明的实施例提供了在分布计算机系统中用于对资源可靠控制存取的改进方法和系统。本发明的一个实施例存储和赋值具有目标对象的组标识，然后使用全体成员核对，以确定以用户名义向目标对象请求存取的客户对象是否是该组成员。这样，本发明就避免了为核实请求对象的存取权所采用的昂贵的加密操作。

本发明的第二实施例向目标对象基准存储和赋值组标识，然后把目标对基准到系统中的客户对象。由于目标对象基准包括组标识入口，因此第一客户对象能够确定系统中的其他客户是该标识组的成员。该确定允许第一客户对象把目标对象基准传到该组的其他成员，而不需要首先与目标对象的服务器联系。这样，本发明就避免了与目标对象的服务器联系的昂贵处理费用。

图1是用于实施本发明的优选实施例的计算机系统100的方框图。计算机系统100包括计算机101、输入装置103、存储装置105、和显示装置107。 显示装置107显示图示用户接口(GUI)109。该GUI通过图标呈现信息并且用户通过指出或操纵该图标来行使命令。计算机101包括处理器111、存储器113、 和在处理器111与图示装置之间能够进行联系的接口115，所述的图示装置是像输入装置103和显示装置107那样的装置。

计算机存储器含有包括客户对象117、混合文件服务器对象119和伸展服务器对象121。存储器113的内容将在下面详细描述。

本发明的各种实施例通过举例进行最好的说明。下面的两个实施例将在建立和印制混合文件的上下文中讨论。混合文件一般包括正文和图形。例如，包括年销售增长的图表、曲线和说明正文的年度销售报告作为混合文件被制成。通常，在混合文件服务器控制下存储混合文件时，图表和曲线在伸展图表服务器的控制下同图表和曲线的连接指令一起被存储。

尽管本发明的实施发生在属于一个计算机的不同流程之间， 但本领域的普通技术人员将会明白这里的说明同样适用于分布在整个网络设施的对象和流程。

当流程开始于两个实施例之前， 一定的先决条件应存在于计算机系统100中。这里假定用户（或"委托人"）已成功地存入和已获得系统100 的凭证和已请求了客户对象117。在本实例中，客户对象117一般与包含字处理申请的处理相适应。为了指示对象117足以委托人的名义起作用， 委托人凭证存有客户对象117。此外，在计算机系统100上，委托人与具有存取特权的一组其它委托人相关联。例如，销售员能与作为销售部门的组相关联。限定在系统100 中的每个组具有与其相关的特殊组标志符。此外，用于核对全体成员凭证的机构（即机构123）应该被给出， 以确定是以委托人的名义还是以特定组的成员名义对一对象起作用。用于实现全体成员机构的任何已知的方法或系统都可以实现系统100的这一方面内容。

图2是说明用于对系统资源可靠存取的第一实施例的优选步骤的流程图。图2的步骤一般响应于用户输入的起始。假设委托人启动客户117的请求以建立展开图表（步骤201）。响应该输入，客户对象117把建立请求送到展开图表服务器对象（步骤203）。该请求表明伸展图表对象应该举例说明。 该请求还包括以与混合文件服务器名义操作相关联的组标志符。

伸展图表服务器对象接收该请求并建立伸展图表对象（步骤205）。 伸展图表服务器对象随后存储具有伸展图表对象的组标志符以及关于伸展图表对象的组成员的存取权指示（步骤207）。最后， 伸展图表服务器对象产生不会伪造的数字并存储具有伸展图表对象的不会伪造的数字（步骤209）。这样， 当对服务器对象请求存取的客户对象呈现不会伪造的数字时，伸展图表服务器对象就可以确信该请求的客户有存取伸展图表对象的权力。该不会伪造的数字经常称之为"能力"。一不会伪造的数字是难以计算确定的。

伸展图表服务器对象然后把伸展图表基准送到客户对象117(步骤211)。在该优选实施例中，伸展图表对象包括在先产生的不会伪造的数字。

一旦伸展图表服务器返回对客户对象的操作控制，客户对象就会发现在组中以委托人名义操作的混合文件服务器(步骤213)。接着， 客户对象把建立混合文件的请求送到混合文件服务器119(步骤215)。该建立的请求包括混合文件建立的指示。该建立的请求还包括伸展图表对象基准以便混合文件服务器知道伸展图表对象引入它的混合文件。最后，该建立的请求包括被选择的组标志符以便混合文件服务器可以稍后确定对混合文件请求存取的委托人是否有权存取混合文件。

混合文件服务器建立混合文件并在混合文件中存储伸展图表基准和组标志符(步骤217)。然后， 混合文件服务器产生不会伪造的数字并存储具有混合文件对象的不会伪造的数字。这样，当由对混合文件对象请求存取的客户对象呈现不会伪造的数字时，混合文件服务器对象就会有某种把握确信该请求客户有存取混合文件对象的权力。

混合文件服务器对象119然后把混合文件对象基准送到客户对象117( 步骤219)。在该优选实施例中，混合文件对象基准包括由混合文件服务器对象产生的不会伪造的数字。

在某些稍后的时刻客户对象把打印请求送到混合文件服务器(步骤221) 。打印请求把混合文件基准和客户委托人的识别传送到混合文件服务器。客户使用任何已知鉴别机构以证明有权以客户委托人名义操作的混合文件服务器。靠把混合文件基准和客户委托人的识别传送到混合文件服务器，混合文件服务器就能够确定打印哪个混合文件并通过鉴定识别属于建立混合文件时指定组的核对以及通过比较对象基准中不会伪造数字与对象中的不会伪造数字就能够证实客户对象117允许打印混合文件。 并且将在对象参考中的不会伪造数字与在该对象中的不会伪造数字比较。

为了打印混合文件，混合文件服务器需要有与伸展图表对象关联的数据。所以，混合文件服务器把取得数据请求送到伸展图表服务器(步骤223)。 该取得数据请求包括伸展图表对象基准以便伸展图表服务器从其检索的数据中知道其伸展图表对象。该取得数据请求还包括那些以混合文件服务器名义操作的委托人识别。

混合文件服务器将向伸展图表服务器证实它自己(步骤225)。 证实委托人的任何已知技术可以用于实现申请人实施例的这方面内容。如果混合文件服务器被成功地证实，那么伸展图表服务器就试图确定混合文件服务器是否有允许它从伸展图表对象检索数据的存取权。为确定存取权，伸展图表服务器从伸展图表对象中检索组标志符。伸展图表服务器然后把组标志符和证实委托人标志符以及确定被证实的委托人是否具有伸展图表对象存取权的组成员的请求送到全体成员机构123(步骤227)。任何已知的用于核对组成员的机构可用于实现申请人实施例的这一方面内容。

如果混合文件服务器被证实委托人是指定组的成员，那么伸展图表服务器进行另一个核查以确定混合文件有权存取伸展图表对象。伸展图表服务器从伸展图表服务器基准中检索不会伪造数字并将其与存有伸展图表服务对象的不会伪造数字进行比较(在最佳实施例中该步骤应最好首先实现)(步骤229)。 如果这些不会伪造数字一致，那么伸展图表服务器允许混合文件服务器在存有对象的存取权控制下从伸展图表对象中检索所需数据。

一旦伸展图表数据被检索，混合文件服务器就把混合文件数据送到用于打印的打印服务器(步骤233)。

与第一实施例相关联的好处之一是不需要用加密操作去确定正在请求对象存取的客户是否授权存取对象。与之相反，第一实施例是靠保持伸展图表对象状态数据中的组标志符和然后使用该组标志符去确定请求的客户是否以适当组的成员的用户的名义操作来完成这个授权核对。核对这个组全体成员一般来说比用加密操作费用低。

第一实施例的另一个优点是伸展图表服务器可以确定谁有对恰好使用保持在伸展图表对象上的状态数据给定对象的存取。在别的现有技术中，完成这一切是不可能的，因为只有对象基准存储了存取权信息。存取权信息不存有对象本身。

图3 是说明用于可靠控制对系统资源的存取的第二实施例的优选步骤的流程图。 图3 的步骤一般响应用户输入而启动。 假定委托人启动客户117 的请求以建立伸展图表 (步骤301)。 响应该输入， 客户对象117 把建立请求送到伸展图表服务器对象 (步骤 303 )。 该请求表明伸展图表对象应该对实例说明。该请求还包括与那些以混合文件服务器名义操作的委托人相关联的组标志

符。

伸展图表服务器对象接收该请求和建立伸展图表对象(步骤305)。然后，伸展图表服务器对象把伸展图表对象基准送给客户对象117。在第二实施例中，伸展图表对象基准包括随建立请求送来的组标志符、 指示该组的存取权特权的入口、和伸展图表对象标志符。伸展图表对象基准可以是遍及密码方式的杂乱信号函数，在对象基准数据上产生密码检查和。该密码检查和还保存在伸展图表对象基准中或与伸展图表对象基准相关联。

一旦伸展图表服务器把流程控制返回到客户对象，客户对象就把建立混合文件的请求送给混合文件服务器119(步骤309)。该建立请求包括混合文件应被建立的指示。该建立请求还包括伸展图表对象基准以便混合文件服务器知道引入它的混合文件的哪个伸展图表对象。该建立请求进一步包括选择组标志符以便混合文件服务器可以确定代表向混合文件请求存取的某些委托人的对象操作是否授权存取混合文件。

混合文件服务器建立混合文件和在混合文件中存储伸展图表基准(步骤311)。然后，混合文件服务器对象119送给客户对象117一个混合文件对象基准(步骤313)。在第二个实施例中，混合文件对象基准包括组标志符、表明组中那些存取权的入口、混合文件的标志符和在混合文件基准建立期间由混合文件服务器产生的密码检查和。

在稍后时刻，客户对象把打印请求送给混合文件服务器(步骤315)。 打印请求把混合文件基准和客户委托人的识别传给混合文件服务器。该客户使用任何已知鉴别机构去证实有权代表客户委托人操作的混合服务器(步骤317)。 这样，混合文件服务器靠使用下面详细描述的密码检查和就明白打印哪个混合文件和可以检验客户对象117有打印混合文件的许可。

为了打印混合文件，混合文件器需要有与伸展图表对象相关联的数据。所以，混合文件服务器把取得数据请求送给伸展图表服务器(步骤319)。 该取得数据请求包括伸展图表对象基准，以便伸展图表服务器知道来自哪个检索数据的伸展图表对象。该取得数据请求还包括代表混合文件服务器操作的委托人识别。

伸展图表服务器鉴别混合文件服务器(步骤321)。 任何鉴别委托人的已知技术可以实现申请人的第二实施例的这方面内容。如果混合文件服务器被成功

地鉴别，那么伸展图表服务器就试图确定混合文件服务器是否有允许它从伸展图表对象中检索数据的存取权(步骤323)。为确定存取权，伸展图表服务器检索与伸展图表对象基准相关联的组标志符。然后，伸展图表服务器从伸展图表对象基准中检索伸展图表标志符。最后，伸展图表服务器把检索信息以及确定被鉴别委托人是否是具有对伸展图表对象存取权的识别组的一个成员的请求送给全体成员机构123。任何用于核对组全体成员的已知机构可以实现申请人的第二实施例的这方面内容。

如果被鉴别委托人是识别组的一个成员，那么伸展图表服务器就进行另一个核对以确信混合文件被授权去存取伸展图表对象。伸展图表服务器从伸展图表基准中检索密码检查和，然后再次计算伸展图表对象的密码检查和（步骤325)。接着，伸展图表服务器把检索的检查和与再次计算的检查和进行比较（步骤327)。如果这些检查和一致，那么伸展图表服务器允许混合文件服务器在对象基准中的存取权控制下从伸展图表对象中检索所需的数据。

一旦检索伸展图表数据，混合文件服务器就把混合文件数据送给用于打印的打印服务器(步骤329)。

第二实施例的优点之一是：靠保持有关为使用对象基准而授权的那个组和那些其它成员处于该组中的状态，使客户对象可以把与该组相关联的该对象基准传给该组中的另一个委托人，而不需要进行与服务器的任何信息交流。避免这种与伸展图表服务器的联系能改善性能和效率。

尽管用于说明目的的本发明特定实施例已经进行了说明，但在不背离本发明精神和范围的前题下可以作出各种变形。所以本发明不限于上述的实施例。

例如，根据由熟悉当前技术的人员广泛理解的技术通过一些方式可以改进两种实施例。在第一种实施例中，组标志符也许不仅存储在对象中，而且还与作为线索的对象基准一同送给客户。第一客户可以核对第二顾客存在于组中。没有这个线索，第一顾客就必须请求来自服务器的组标志符，以请求信息交流。

在第二实施例中，当对象基准被提出使用时，服务器就可以超高速缓存具有该对象的对象基准。接着，服务器可以用超高速缓存器中的内容核对客户送入的对象基准。这意味着如果对象基准由同一组中不同客户提出，服务器就不

需要再计算密码检查和。这样，用于那些存取的服务器可以减少计算，从而增强了本发明的性能。

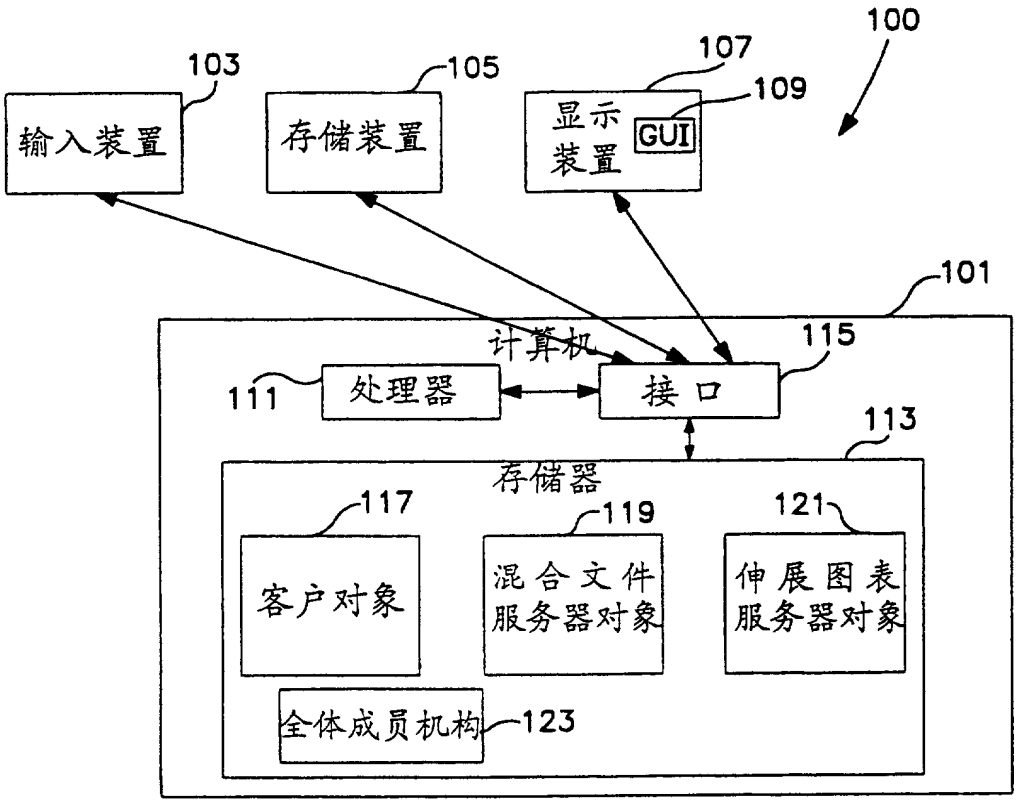

100
103
输入装置
105
存储装置
107
显示装置
109
GUI
101
计算机
115
111
处理器
接口
113
存储器
117
客户对象
119
混合文件服务器对象
121
伸展图表服务器对象
全体成员机构
123

图 1

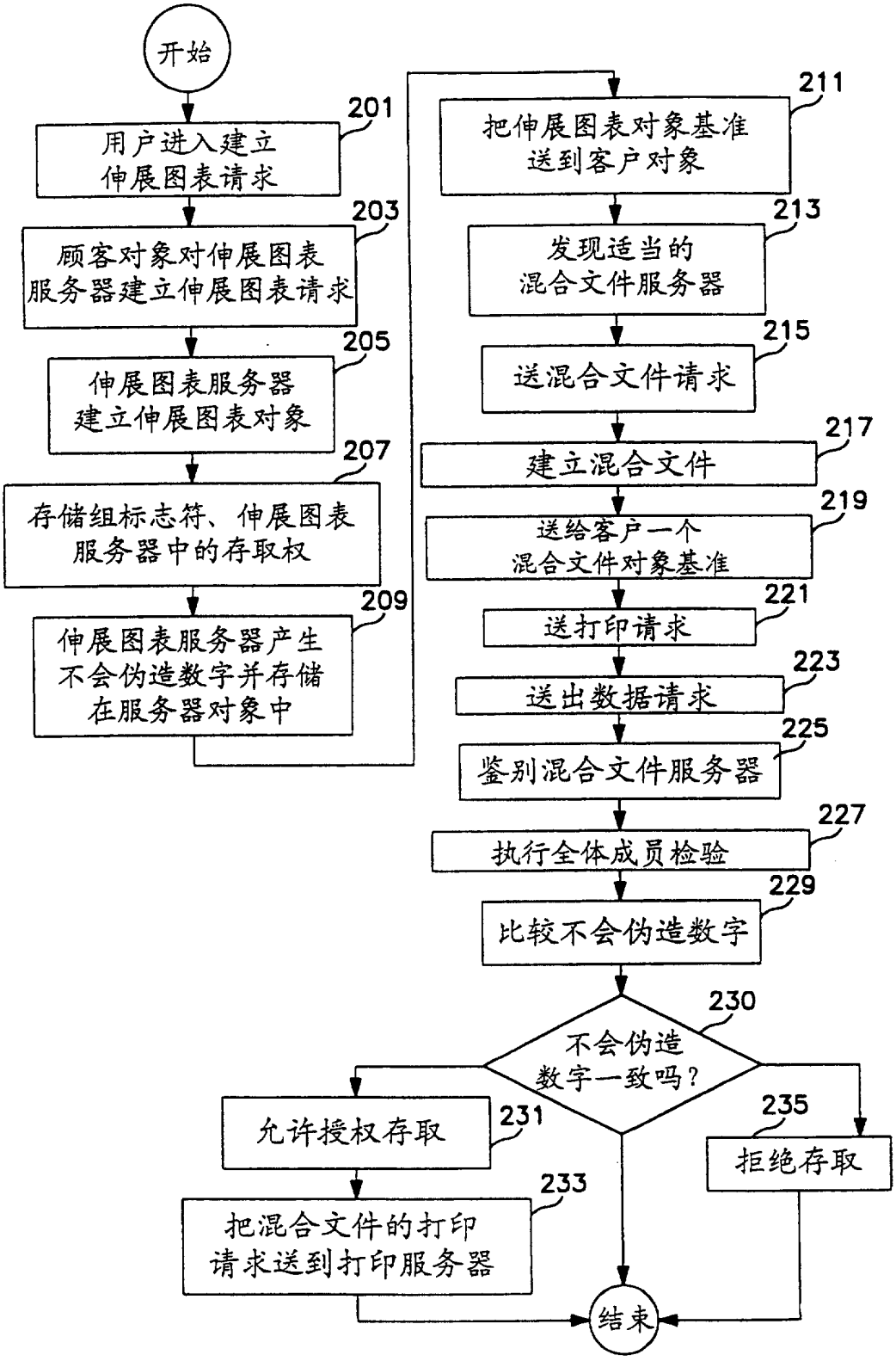

开始
201
用户进入建立伸展图表请求
203
顾客对象对伸展图表服务器建立伸展图表请求
205
伸展图表服务器建立伸展图表对象
207
存储组标志符、伸展图表服务器中的存取权
209
伸展图表服务器产生不会伪造数字并存储在服务器对象中
211
把伸展图表对象基准送到客户对象
213
发现适当的混合文件服务器
215
送混合文件请求
217
建立混合文件
219
送给客户一个混合文件对象基准
221
送打印请求
223
送出数据请求
225
鉴别混合文件服务器
227
执行全体成员检验
229
比较不会伪造数字
230
不会伪造数字一致吗?
231
允许授权存取
233
把混合文件的打印请求送到打印服务器
235
拒绝存取
结束

图 2

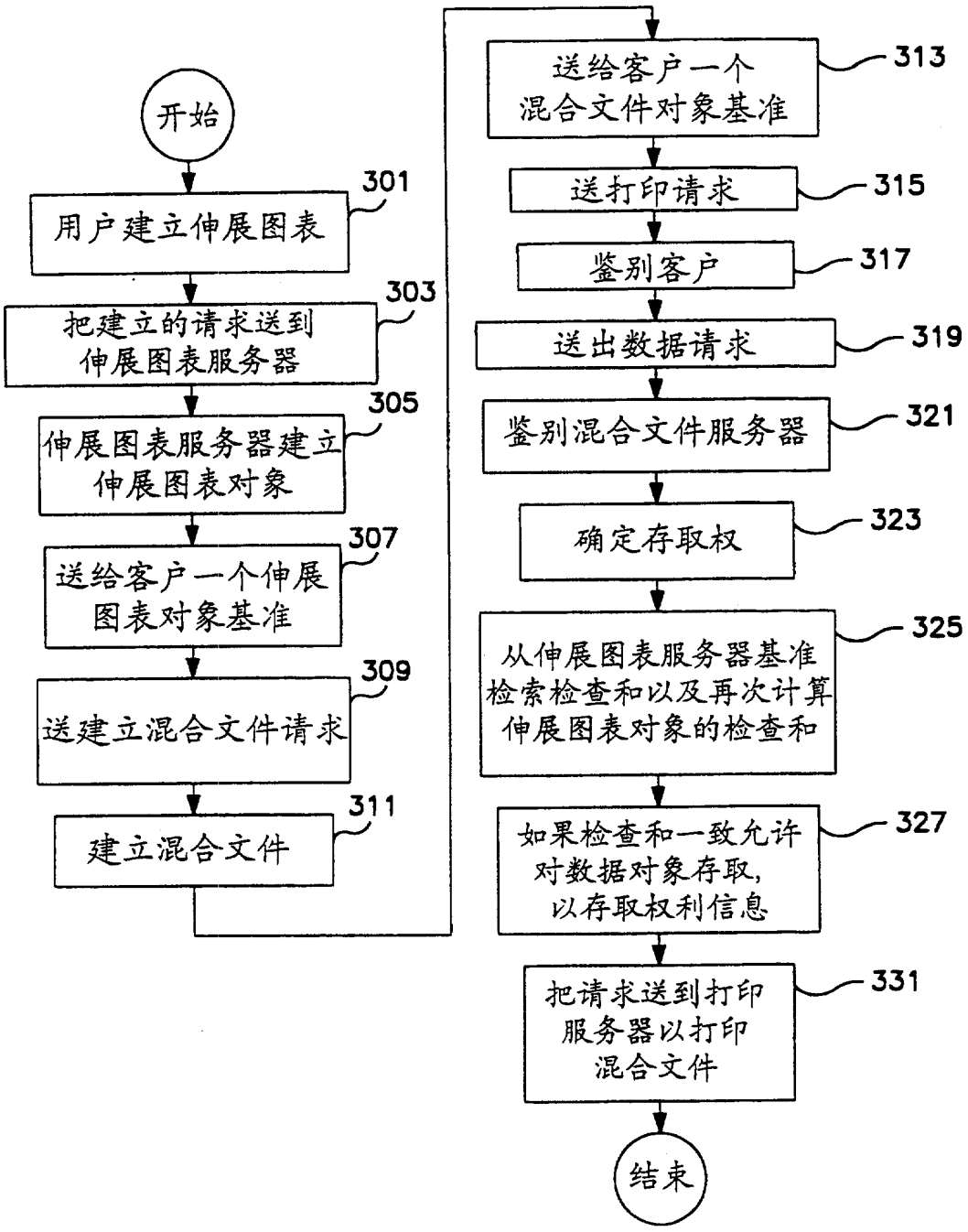

开始
用户建立伸展图表
301
把建立的请求送到伸展图表服务器
303
伸展图表服务器建立伸展图表对象
305
送给客户一个伸展图表对象基准
307
送建立混合文件请求
309
建立混合文件
311
送给客户一个混合文件对象基准
313
送打印请求
315
鉴别客户
317
送出数据请求
319
鉴别混合文件服务器
321
确定存取权
323
从伸展图表服务器基准检索检查和以及再次计算伸展图表对象的检查和
325
如果检查和一致允许对数据对象存取，以存取权利信息
327
把请求送到打印服务器以打印混合文件
331
结束

图 3