

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/24 (2006.01)

H04L 9/32 (2006.01)



# [12] 发明专利说明书

专利号 ZL 200510078977.6

[45] 授权公告日 2008年7月2日

[11] 授权公告号 CN 100399749C

[22] 申请日 2005.6.21

[21] 申请号 200510078977.6

[30] 优先权

[32] 2004.8.26 [33] US [31] 10/926,550

[73] 专利权人 国际商业机器公司

地址 美国纽约

[72] 发明人 谭逸心 王守慧

[56] 参考文献

CN1507732A 2004.6.23

CN1453954A 2003.11.5

CN1338845A 2002.3.6

WO2004/059942A1 2004.7.15

CN1464715A 2003.12.31

WO03/084152A1 2003.10.9

US2003/0200443A1 2003.10.23

审查员 李 燕

[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

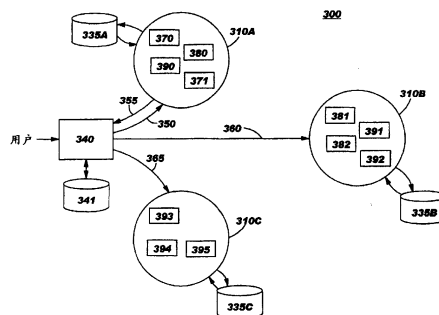
权利要求书 3 页 说明书 12 页 附图 6 页

[54] 发明名称

用于聚集系统中的用户授权级别的方法和系统

[57] 摘要

通过基于与用户相关联的不同聚集授权级别而授权对来自包括在服务提供者聚集系统中的不同服务提供者的不同服务的访问，可以在连网应用服务环境中提供服务。还公开了相关的系统和计算机程序产品。



1. 一种在连网应用服务环境中提供服务的方法，包括：

由服务提供者聚集系统中的服务提供者确定与用户相关联的不同聚集授权级别；以及

基于所述与用户相关联的不同聚集授权级别，授权对来自包括在服务提供者聚集系统中的所述服务提供者以及其他服务提供者的不同服务的访问。

2. 根据权利要求 1 所述的方法，其中授权还包括：

基于第一授权级别而允许对来自服务器的第一服务的访问并且禁止对来自服务器的第二服务的访问；以及

基于第二授权级别而允许对来自服务器的第二服务的访问。

3. 根据权利要求 2 所述的方法，其中第一授权级别包括从本地系统授权级别映射的聚集系统中的聚集系统授权级别。

4. 根据权利要求 2 所述的方法，其中第一服务包括基于第一授权级别而可被用户访问的第一应用，并且第二服务包括基于第二授权级别而可被用户访问的第二应用。

5. 根据权利要求 1 所述的方法，其中授权还包括：

基于第一授权级别而允许对来自服务器的服务的只读访问；以及

基于第二授权级别而允许对来自服务器的服务的读/写访问。

6. 根据权利要求 1 所述的方法，其中不同服务包括基于与用户相关联的授权级别而可被用户访问的不同应用。

7. 根据权利要求 1 所述的方法，其中在访问之前执行授权。

8. 根据权利要求 1 所述的方法，其中授权包括响应用户通过聚集系统的接口的访问而将用于访问该系统中的服务的授权级别与认证一起提供给该接口。

9. 根据权利要求 8 所述的方法，其中响应来自接口的单个认证请求，将授权级别和认证提供给接口。

10. 根据权利要求 1 所述的方法，由在计算机可读介质中实施的计

计算机程序产品执行。

11. 一种在连网应用服务环境中提供服务的服务提供者聚集系统，包括：

服务提供者，该服务提供者确定与用户相关联的不同聚集授权级别；以及用于基于所述与用户相关联的不同聚集授权级别而授权对来自包括在服务提供者聚集系统中的所述服务提供者以及其他服务提供者的不同服务的访问的装置。

12. 一种在连网应用服务环境中提供服务的方法，包括：

从与服务提供者聚集系统的接口接收用户的认证请求；

确定与该用户相关联的用来访问聚集系统中的服务的授权级别；以及

将该用户的用户认证和与该用户相关联的授权级别提供给接口。

13. 根据权利要求 12 所述的方法，其中授权级别包括对通过聚集系统中的第一服务提供者可用的第一应用的第一授权级别、以及对通过聚集系统中的第二服务提供者可用的第二应用的第二授权级别。

14. 根据权利要求 13 所述的方法，其中第一授权级别包括对第一应用的只读访问，并且第二授权级别包括对第二应用的读/写访问。

15. 一种在连网应用服务环境中提供服务的方法，包括：

在包括来自服务提供者的可用的服务的提供者聚集系统中注册服务提供者；

在与聚集系统的接口处从用户接收用于访问服务提供者聚集系统的请求；

向包括在聚集系统中的具有与该用户相关联的简档的服务提供者请求对该用户的认证和与该用户相关联的授权级别；以及

接收对用户的认证和与该用户相关联的授权级别。

16. 根据权利要求 15 所述的方法，还包括：

基于与服务提供者相关联的用户订购，在服务提供者处确定用户的授权级别，以表明聚集系统中的哪些服务可被该用户访问；以及

根据授权级别允许通过接口对服务的访问。

17. 根据权利要求 15 所述的方法，还包括：

将在聚集系统中可用的不同授权级别从接口提供给服务提供者；以及

在服务提供者处确定不同授权级别中的哪个适用于该用户，以表明聚集系统中的哪些服务可被该用户访问。

18. 一种用于在连网应用服务环境中提供服务的系统，包括：

用于在包括来自服务提供者的可用的服务的服务提供者聚集系统中注册服务提供者的装置；

用于在与聚集系统的接口处从用户接收用于访问服务提供者聚集系统的请求的装置；

用于向包括在聚集系统中的具有与该用户相关联的简档的服务提供者请求对该用户的认证和与该用户相关联的授权级别的装置；以及

用于接收对用户的认证和与该用户相关联的授权级别的装置。

## 用于聚集系统中的用户授权级别的方法和系统

### 技术领域

本发明涉及用于处理信息的方法、系统和计算机程序产品，特别涉及用于在连网计算机环境中处理信息的方法、系统和计算机程序产品。

### 背景技术

公知的是，通过单点“登录”提供聚集服务，其中用户可以在通过登录使他们的身份被认证之后访问服务。这里所使用的术语“被认证”是指确定用户是他/她被声称使用例如与用户相关联的用户名和密码的人。然而，在一些单点登录聚集系统中，在可使用服务之前，可能仍然需要用户单独地获得对由聚集系统提供的每一个服务的访问。例如，如果用户登录聚集系统以访问由两个不同的服务提供者提供的两个不同服务，则可通过登录来认证用户，但是用户可能仍然需要通过将另外的信息提供给这两个服务的一个或另一个来获得对访问这些服务的授权。

这样的上述单点登录聚集系统的两个例子是由微软公司，雷德蒙，华盛顿提供的.NET 通行证系统(“Passport”)和由太阳微系统公司，芒廷维，加利福尼亚提供的自由联盟系统(“Liberty”)。通行证系统提供了通过创建一组凭证来认证用户，其中这组凭证允许用户登录到支持通行证服务的任何服务(例如，由网站提供的服务)。图 1 示出了通行证系统的示例图，其包括通行证服务器 115 和三个服务提供者 110A-C，其中每一个服务提供者支持通行证系统 100。根据图 1，通过在链路 105 上登录服务提供者 110A，用户可使用例如计算机 101 访问通行证系统。服务提供者 110A 通过链路 120 将用户的登录重定向到通行证服务器 115，由此用户登录到通行证服务器 115。通行证服务器 115 可使用在本地可访问的用户身份信息 130 认证用户的登录信息。如果用户的登录信息被认证，则通过链路 135 将用户从通行证服务器 115 重定向回到服务

提供者 110A, 由此服务提供者 110A 允许用户访问在其上提供的服务。应当理解, 服务提供者 110B 和 C 可以类似地工作。

图 2 示出了自由联盟系统的示例图, 其包括服务提供者 210A-C 和身份服务器 214。具体地说, 用户可使用例如计算机 201 在链路 205 上通过自由联盟系统 200 对服务提供者 210A 访问服务。用户对服务提供者 210A 的登录通过链路 220 被重定向到身份服务器 214, 由此用户使用可用于身份服务器 214 的身份信息 230 登录。身份服务器 214 使用身份信息 230 以确定(由身份信息 206A-C 标识的)用户是否是链路 222 上的服务提供者 210A、链路 223 上的服务提供者 210B、或者链路 224 上的服务提供者 210C 所知道的真实用户。如果身份服务器 214 能够验证用户的真实性, 则通过链路 235 将用户重定向回到服务提供者 210A, 由此用户能够通过服务提供者 210A 访问服务。

尽管存在由诸如通行证和自由联盟的聚集系统提供的认证服务, 但是需要进一步改善通过聚集系统提供认证和授权透明服务。聚集系统中的每个服务提供者未必知道授权级别、用户身份和由其他服务提供者提供的服务。从而, 可能难以以适当的粒度级别授权向一个服务提供者订购的用户使用由其他服务提供者提供的服务。

### 发明内容

根据本发明的实施例可提供用于聚集系统中的用户授权级别的方法、系统和计算机程序产品。根据这些实施例, 通过基于与用户相关联的不同聚集授权级别而授权对来自包括在服务提供者聚集系统中的不同服务提供者的不同服务的访问, 可执行一种在连网应用服务环境中提供服务的方法。

在根据本发明的一些实施例中, 授权还可包括基于第一授权级别而允许对来自服务器的第一服务的访问并且禁止对来自服务器的第二服务的访问, 以及基于第二授权级别而允许对第二服务的访问。在根据本发明的一些实施例中, 第一授权级别可以是本地系统授权级别映射的聚集系统中的聚集系统授权级别。

在根据本发明的一些实施例中，第一服务可以是基于第一授权级别而可被用户访问的第一应用，并且第二服务可以是基于第二授权级别而可被用户访问的第二应用。

在根据本发明的一些实施例中，授权还可包括基于第一授权级别而允许对来自服务器的服务的只读访问，并且基于第二授权级别而允许对来自服务器的服务的读/写访问。

在根据本发明的其他实施例中，不同服务可以是基于与用户相关联的授权级别而可被用户访问的不同应用。在根据本发明的另外实施例中，在由用户访问之前执行授权。

在根据本发明的其他实施例中，授权可包括响应通过聚集系统的接口由用户访问而将用于访问该系统中的服务的授权级别与认证一起提供给该接口。在根据本发明的其他实施例中，响应来自接口的单个认证请求，将授权级别和认证提供给接口。

在根据本发明的其他实施例中，通过从与服务提供者聚集系统的接口接收认证用户的请求，可提供在连网应用服务环境中提供服务的方法。可确定与用户相关联的用来访问聚集系统中的服务的授权级别。可将对用户的用户认证和与其相关联的授权级别提供给接口。

在根据本发明的其他实施例中，授权级别可以是对通过聚集系统中的第一服务提供者可用的第一应用的第一授权级别、以及对通过聚集系统中的第二服务提供者可用的第二应用的第二授权级别。在根据本发明的其他实施例中，第一授权级别可以是对第一应用的只读访问，并且第二授权级别可以是对第二应用的读/写访问。

在根据本发明的一些实施例中，在连网应用服务环境中提供服务的方法可包括在包括从服务提供者可用的服务的提供者聚集系统中注册服务提供者。可在与聚集系统的接口处从用户接收用于访问服务提供者聚集系统的请求。可向包括在聚集系统中的具有与用户相关联的简档(profile)的服务提供者请求对用户的认证。可接收对用户的认证和与其相关联的授权级别。

## 附图说明

图 1 是通行证系统的示例图。

图 2 是自由联盟系统的示例图。

图 3 是根据本发明一些实施例的服务提供者聚集系统的示例图。

图 4 是示出根据本发明一些实施例的服务提供者聚集系统的操作的流程图。

图 5 是示出根据本发明一些实施例的由不同用户使用应用的不同授权级别的表。

图 6 是根据本发明一些实施例的访问聚集系统之前的注册过程的示意图。

## 具体实施方式

这里参照附图描述本发明，其中示出了本发明的多个实施例。然而，本发明可采用多种不同形式实施，并且不应当被解释为局限于这里阐述的实施例；相反，提供这些实施例是为了使本公开内容详尽且完整，并且向本领域的技术人员完全传达本发明的范围。相同的标号和附图标记始终表示相同的单元。

本领域的技术人员应当清楚，本发明可被实施为方法、系统和/或计算机程序产品。从而，本发明可采取完全硬件实施例、完全软件实施例或组合软件和硬件方面的实施例的形式。此外，本发明可采取计算机可用存储介质上的计算机程序产品的形式，其中该计算机可用存储介质中实施有计算机可用程序代码。可利用任何适合的计算机可读介质，包括硬盘、CD-ROM、光存储装置或磁存储装置。

用于执行根据本发明的操作的计算机程序代码或“代码”可采用面向对象的编程语言如 JAVA®、Smalltalk 或 C++、JavaScript、Visual Basic、TSQL、Perl 或者各种其他编程语言编写。本发明的软件实施例不依赖于采用特定编程语言的实现。代码的各部分可以完全地在由中间服务器利用的一个或多个系统上执行。

代码可以完全地在一个或多个服务器上执行，或者它可以部分地在



服务器上执行并且部分地在客户端设备内的客户端上执行，或者作为位于通信网络中的中间点的代理服务器执行。在后者场景中，客户端设备可以在 LAN 或 WAN(例如，内联网)上连接到服务器，或者可以通过因特网(例如，因特网服务提供者)来进行连接。应当理解，本发明不是 TCP/IP 特定的或者因特网特定的。本发明可以在各种类型的计算机网络上使用各种协议实施。

下面参照根据本发明实施例的方法、系统和计算机程序产品的方框图和流程图描述本发明。应当理解，方框图和/或流程图中的每个块以及方框图和流程图中的块组合可通过计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机或者其他可编程数据处理设备的处理器，以产生一种机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令创建用于实现在方框图和/或流程图的一个块或多个块中指定的功能的装置。

这些计算机程序指令可被存储在计算机可读存储器中，其可引导计算机或其他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中的指令产生一种包括实现在方框图和/或流程图的一个块或多个块中指定的功能的指令装置的产品。

计算机程序指令可被装载到计算机或其他可编程数据处理设备上，从而致使在计算机或其他可编程设备上执行一系列操作步骤，以产生一种计算机实现的过程，使得在计算机或其他可编程设备上执行的指令提供用于实现在方框图和/或流程图的一个块或多个块中指定的功能的步骤。

这里所使用的术语“服务提供者”可包括通过例如作为网站一部分的网页提供一个或多个服务的服务器。网站可包括多个文件的相关集合，其包括称作主页的开始文件。从主页，用户可访问网站上的其他文件和应用。大的网站可利用多个服务器，其可以是或者可以不是不同的，并且可以是或者可以不是地理上分散的。例如，国际商业机器公司的网站([www.ibm.com](http://www.ibm.com))包括分散在全世界范围的多个位置的多个万维网服务器上的数千网页和文件。

在上述例子中，网页还可以以为独立于 GUI 方法的应用的程序化访问而设置的环境中的万维网服务更替。万维网服务可提供 WSDL、SOAP 和 XML 消息标准，使得程序可访问网站上以这些标准表示的应用。

根据本发明的实施例可在逻辑上分离的客户端侧/服务器侧计算环境中工作，以下有时将客户端侧/服务器侧计算环境称作客户端/服务器环境。客户端/服务器环境是涉及客户端过程(即客户端)向服务器进程(即服务器)请求服务的计算架构。一般而言，虽然客户端和服务器进程可在不同机器上或者在相同机器上工作，但是客户端/服务器环境保持进程间区别。从而，客户端/服务器环境的客户端和服务器侧被称作在逻辑上是分离的。通常，当客户端和服务器进程在单独的设备上工作时，可以针对各自进程的需要定制每个设备。例如，服务器进程可在具有大量存储器和盘空间的系统上“运行”，而客户端进程经常在具有由高端视频卡和大屏幕显示器提供的图形用户界面的系统上“运行”。

客户端可以是在用户的控制下向服务器请求信息如网页的程序如万维网浏览器。客户端的例子包括诸如 Netscape Navigator®(美国在线公司，杜勒斯，弗吉尼亚)和 Internet Explorer®(微软公司，雷蒙德，华盛顿)的浏览器。浏览器典型地提供用于检索和查看由万维网服务器供应的网页、万维网门户、应用和其他资源的图形用户界面。SOAP 客户端可用来代替万维网浏览器由程序以程序化方式请求万维网服务。

由服务提供者提供的应用可在服务器上执行。服务器可以是响应来自客户端的请求的程序。服务器的一些例子是国际商业机器公司的 Lotus Domino®服务器系列、Apache 服务器和微软的因特网信息服务器(IIS)(微软公司，雷蒙德，华盛顿)。

客户端和服务器可使用标准通信模式例如超文本传输协议(HTTP)和 SOAP 通信。根据 HTTP 请求-响应通信模型，将 HTTP 请求从客户端发送到服务器，并且响应 HTTP 请求将 HTTP 响应从服务器发送到客户端。工作时，服务器等待客户端打开连接并请求诸如网页的信息。作为响应，服务器将所请求信息的副本发送到客户端，关闭与客户端的

连接，并且等待下一个连接。在 SOAP 模型中，通过 XML 消息交换来传送请求和响应。应当理解，服务器可响应来自多个客户端的请求。

这里所使用的“聚集系统”包括在其他方面单独的服务提供者所提供的多个服务。在这样的聚集系统中，一旦用户已被认证和授权(如这里更详细描述的那样)，则用户可访问由不同服务提供者提供的服务的一些或全部。例如，聚集系统可以是多个提供医疗研究服务、新闻服务和数据挖掘服务的的服务提供者。应当理解，单独的服务提供者可以是可经历单独的订购服务或者具有单独的管理授权的服务提供者。传统地，用户可能需要被单独授权以访问这些服务的每一个。然而，在聚集系统中，用户可在被授权一次之后访问该系统中的至少一些服务。

如这里更详细描述的那样，根据本发明的实施例可基于与聚集系统的用户相关联的不同聚集授权级别而提供对访问服务提供者聚集系统中的不同服务的授权。例如，在提供不同类型的在线研究工具的聚集系统中，具有第一授权级别的用户可能被给予对包括在聚集系统中的有限数目的应用的访问，而第二用户(具有更高授权级别)可能具有对更多应用的访问。而且，第二应用可具有一些应用中的读/写授权，而第一用户可被限定于只读授权。

在注册过程期间(例如，当将服务添加到聚集系统时)，可分配与用户相关联的不同授权级别。注册过程可涉及与聚集系统的接口和要包括在聚集系统中的每一个服务提供者之间的通信。在根据本发明的一些实施例中，在注册过程期间，与聚集系统的接口可提供在聚集系统内允许的不同授权级别的简档。例如，该接口可向新的服务提供者通知在聚集系统中允许三个不同的授权级别。服务提供者可通过将服务提供者的本地授权级别映射到在聚集系统中提供的不同授权级别而作用于由该接口提供的授权级别。

上面一般描述的这些方案可以允许改善聚集系统上的可扩展性(即，在将新的服务提供者添加到系统的情况下)，并且鉴于可在由用户访问之前发生的注册，由于可减少服务提供者与接口之间的通信而可减小开销。在根据本发明的一些其他实施例中，在注册过程期间，服务提

供者可通知用户简档的接口，并且提供分类映射，以便以后在用户请求对服务的访问时基于提供者向接口返回的身份参数值而分配实际的授权级别。

图 3 是根据本发明一些实施例的包括多个授权级别的服务提供者聚集系统的示例图。具体地说，聚集系统 300 包括服务提供者 310A-C 和聚集系统接口 340，通过该接口，用户可访问聚集系统 300。每一个服务提供者 310A-C 在本地关联了用户身份信息 335A-C，该信息反映通过例如对由服务提供者提供的服务的订购而为各自的服务提供者 310A-C 所知的用户。例如，服务提供者可提供通过订购可用的在线研究工具。而且，不同的订购可隐含着对已知用户或订户的不同授权级别。例如，为服务提供者 310A 所知的第一用户可具有授权用户访问由服务提供者 310A 提供的应用中的仅一个应用的第一授权级别。相反，第二用户可具有高于第一授权级别的第二授权级别，其中第二授权级别授权第二用户访问由服务提供者 310A 提供的所有应用。

工作时，用户可通过接口 340 访问聚集系统 300。根据图 3，用户通过接口 340 登录到聚集系统 300，以访问由聚集系统 300 提供的服务。作为响应，接口 340 向用户与其相关联的服务提供者请求授权级别信息。具体地说，接口 340 可具有对身份信息 341 的访问，其中身份信息 341 表示聚集系统 300 的每一个已知用户与哪些服务提供者相关联以及用户偏好数据。例如，聚集系统 300 的一些用户可具有向服务提供者 310A 的订购，而其他用户可分别具有向服务提供者 310B 和 310C 的订购。

关联的服务提供者通过访问本地授权级别信息 335A-C 而响应授权级别信息请求，并且为请求访问聚集系统 300 的用户确定授权级别。例如，通过链路 350 联系服务提供者 310A，以通过链路 355 向接口 340 提供请求访问的用户的授权级别信息。该授权级别信息可超出传统的读或写访问、管理员或权利用户访问等，因为这样的信息可能不被不同的系统理解。例如，该授权级别信息可包括描述本地用户的特征的元数据，例如所授权服务的类型、技能系列和组织责任。应当理解，用户的

本地授权级别可由接口 340 使用以授权用户访问由聚集系统 300 中的其他服务提供者提供的**应用**。例如，具有适当高的授权级别的用户(向服务提供者 310A 进行了订购的用户)可被允许访问由服务提供者 310B 和 310C 提供的**应用**。应当理解，除了授权级别信息之外，认证信息也可被提供给接口 340。例如，服务提供者 310A 可表示请求对访问服务的授权的用户实际上是服务提供者 310A 的真实订户以及具有与该认证用户的订购相关联的授权级别。

当在接口 340 处接收到授权级别信息时，用户可被授权访问与用户的聚集授权级别相关联的**应用**。例如，根据图 3，如果用户具有第一级授权，则用户可被授权访问通过服务提供者 310A 可用的**应用 370 和 371**，但是不可访问在聚集系统 300 内可用的任何其他**应用**。相反，如果用户具有第二级授权，则用户可被授权访问通过服务提供者 310A 可用的**应用 370、371 和 380**以及通过服务提供者 310B 可用的**应用 381 和 382**。此外，如果用户的授权级别为第三级，则用户可被授权访问通过服务提供者 310A 可用的**应用 370、371、380 和 390**、通过服务提供者 310B 可用的**应用 381、382、391 和 392**、以及通过服务提供者 310C 可用的**应用 393、394 和 395**。应当理解，虽然在图 3 中示出了三个服务提供者，但是在根据本发明一些实施例的聚集系统中可包括更多或更少的服务提供者。

图 4 是示出根据本发明一些实施例的包括多个授权级别的聚集系统的操作的流程图。根据图 4，在由用户访问之前，可发生在聚集系统中注册服务提供者(块 405)。应当理解，当将新的服务提供者添加到聚集系统时，或者当已经包括在聚集系统内的服务提供者具有更新的信息例如现在通过聚集系统可用于访问的新**应用**时，可发生服务提供者的注册。

在注册期间提供的信息可通过与聚集系统的接口允许服务提供者(以及在其上提供的**服务**)可被用户访问。如这里所讨论的那样，在根据本发明的一些实施例中，用户的授权级别由服务提供者所返回的与在注册的时候指定的分类授权参数值比较的身份信息确定，或者在根据本发

明的其他实施例中，聚集系统可提供服务提供者以后可用来将本地授权级别映射到聚集系统授权级别的预定授权级别。

聚集系统通过与聚集系统的接口接收访问服务的请求(块 410)。如这里所讨论的那样，该接口可具有本地访问以识别包括每一个关联服务提供者的已知用户的信息。身份信息可以例如在用户认证过程期间从服务提供者获得。身份信息还可包括用户偏好数据例如优选语言、组织信息，例如用户被雇用在哪些部门或组织内、工作分类信息、以及也可作为用户认证过程的一部分提供的其他类型的信息。

当接收到访问请求时，与聚集系统的接口可向与用户相关联的服务提供者请求授权信息和/或认证(身份)信息(块 415)。如这里所述，服务提供者可基于在本地可用于服务提供者的授权级别信息和所提供的聚集系统授权级别而确定授权级别。授权级别信息可基于用户向服务提供者的订购，其可授权用户使用与服务提供者相关联的应用的一些或全部，而且可向用户提供进一步的授权级别，例如对特定应用的只读或读/写授权级别。

服务提供者将授权级别信息和/或认证信息发送到接口，该接口基于所提供的授权级别或身份信息而授权用户访问聚集系统中的服务(块 420)。如这里所述，与不同用户相关联的不同授权级别可允许一些用户访问不可用于具有较低授权级别的用户的用户的应用。此外，具有相对较高授权级别的一些用户可具有读/写授权以例如修改或更新通过应用之一而访问的数据。

图 5 是示出根据本发明一些实施例的不同用户的不同授权级别的示例表。根据图 5，(来自一个服务提供者的)用户 A、B 和 C 各自具有不同的授权级别，其授权用户访问包括在例如图 3 所示的聚集系统内的不同应用。而且，每个授权级别包括特定于包括在聚集系统中的每一个应用的授权级别。例如，用户 A 具有关联的授权级别“1”，其授权用户 A 访问组 1 即通过图 3 所示的服务提供者 310A 可用的应用 370 和 371。而且，用于访问这些应用的用户 A 的授权被限定于只读。从而，用户 A 只可查看通过服务提供者 310A 上的应用 370 和 371 访问的数据。

相反，用户 B 具有授权级别“2”，其授权用户 B 访问组 1 即通过服务提供者 310A 可用的应用 370 和 371。如图 3 所示，用户 B 也被授权访问组 2 即通过服务提供者 310B 可用的应用 380、381 和 382。此外，用户 B 的授权级别允许通过应用 370 和 371 对数据的读/写访问，而对应用 380、381 和 382 的访问被限定于只读。

与用户 A 和 B 相反，用户 C 具有相对高的授权级别(“3”)，其授权用户 C 访问上面关于用户 A 和 B 所述的所有应用、以及组 3 即通过服务提供者 310B 可用的应用 391 和 392 和通过服务提供者 310C 可用的应用 393、394 和 395。此外，用户 C 的授权级别还允许用户 C 读取和写入通过这些应用的任一个访问的任何数据。因此，如上所述，基于与用户相关联的不同授权级别，不同的授权级别可授权不同用户具有对不同服务的访问。

如上所述，在由用户访问聚集系统之前，服务提供者可经历注册过程，由此可预先从服务提供者对所有用户分类地确定授权级别，使得例如可减少关于授权级别和认证的通信。根据图 6，聚集系统 600 包括与其的接口 640 和可提供应用以由聚集系统 600 的用户访问的服务提供者 610A-C。此外，每一个服务提供者 610A-610C 具有对与各自的服务提供者相关联的用户的本地身份信息的访问。例如，每一个服务提供者可提供独立的服务(除了成为聚集系统 600 的一部分之外)，使得用户可向服务提供者订购，因此可通过接口 640 访问聚集系统 600。

在根据本发明的一些实施例中，在注册过程期间，服务提供者 610A-C 提供从每一个各自的服务提供者可用的应用列表以及用于确定可与对这些应用的访问相关联的授权级别的因素。例如，服务提供者 610A 可以随同授权用户访问这些应用的不同授权级别包括读/写或只读类型授权级别一起提供从其可用的服务列表。从而，在注册过程期间，服务提供者 610A-C 可提供各自的服务提供者支持哪些聚集授权级别，以及每一个授权级别特定地授权关联的用户在聚集系统 600 内做什么操作。例如，如果服务提供者 610A 支持聚集授权级别“1”、“2”和“3”，则服务提供者 610A 可在授权级别信息中表明级别“1”授权对特定类型的可

用应用的只读访问，级别“2”授权以不同的只读和读/写授权级别访问在服务提供者 610A 和 610B 上可用的特定类型的应用，并且级别“3”授权用户以读/写授权级别访问通过服务提供者 610A-C 可用的全部应用。

在根据本发明的其他实施例中，接口 640 向服务提供者提供在聚集系统 600 内识别的预定授权级别。因此，在完成注册时，每一个服务提供者 610A-C 包括对于访问聚集系统 600 的用户有效的任何授权级别的列表。工作时，当用户访问聚集系统 600 时，接口 640 向与请求访问的用户相关联的各个服务提供者 610A-C 请求授权信息。作为响应，服务提供者 610A-C 可将与用户相关联的身份信息映射到注册过程期间由接口 640 提供的预定授权级别之一。应当理解，这种注册过程中的授权级别可用来提供这里描述的功能。

如这里所述，根据本发明的实施例可基于与聚集系统的用户相关联的不同聚集授权级别而提供对访问服务提供者聚集系统中的不同服务的授权。例如，在提供不同类型的在线研究工具的聚集系统中，具有第一授权级别的用户可能被给予对包括在聚集系统中的有限数目的应用的访问，而第二用户(具有较高授权级别)可能具有对更多应用的访问。而且，第二用户可具有一些应用中的读/写授权，而第一用户可被限定于只读授权。

在给出本公开内容的优点的情况下，本领域的普通技术人员可进行各种变更和修改而不脱离本发明的精神和范围。因此，必须理解，所示实施例仅是为了示例的目的而阐述的，并且其不应当被认为是限制由所附权利要求限定的本发明。因此，所附权利要求应当被阅读成不仅包括在字面意义上阐述的单元的组合，而且包括用于以基本上相同的方式执行基本上相同的功能以获得基本上相同的结果的所有等效单元。因此，权利要求应当被理解成包括上面具体图示和描述的内容，在概念上相同的内容以及包括本发明的基本思想的内容。



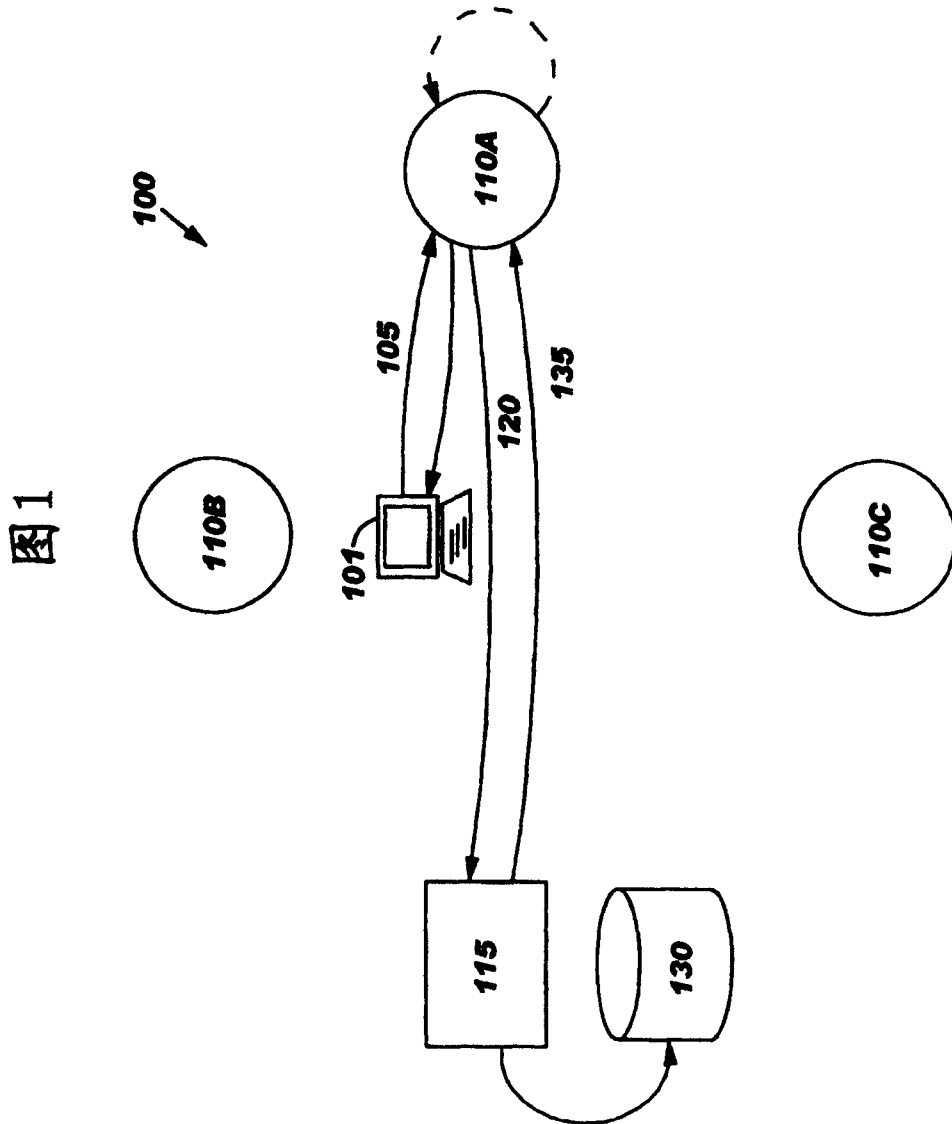




图 3

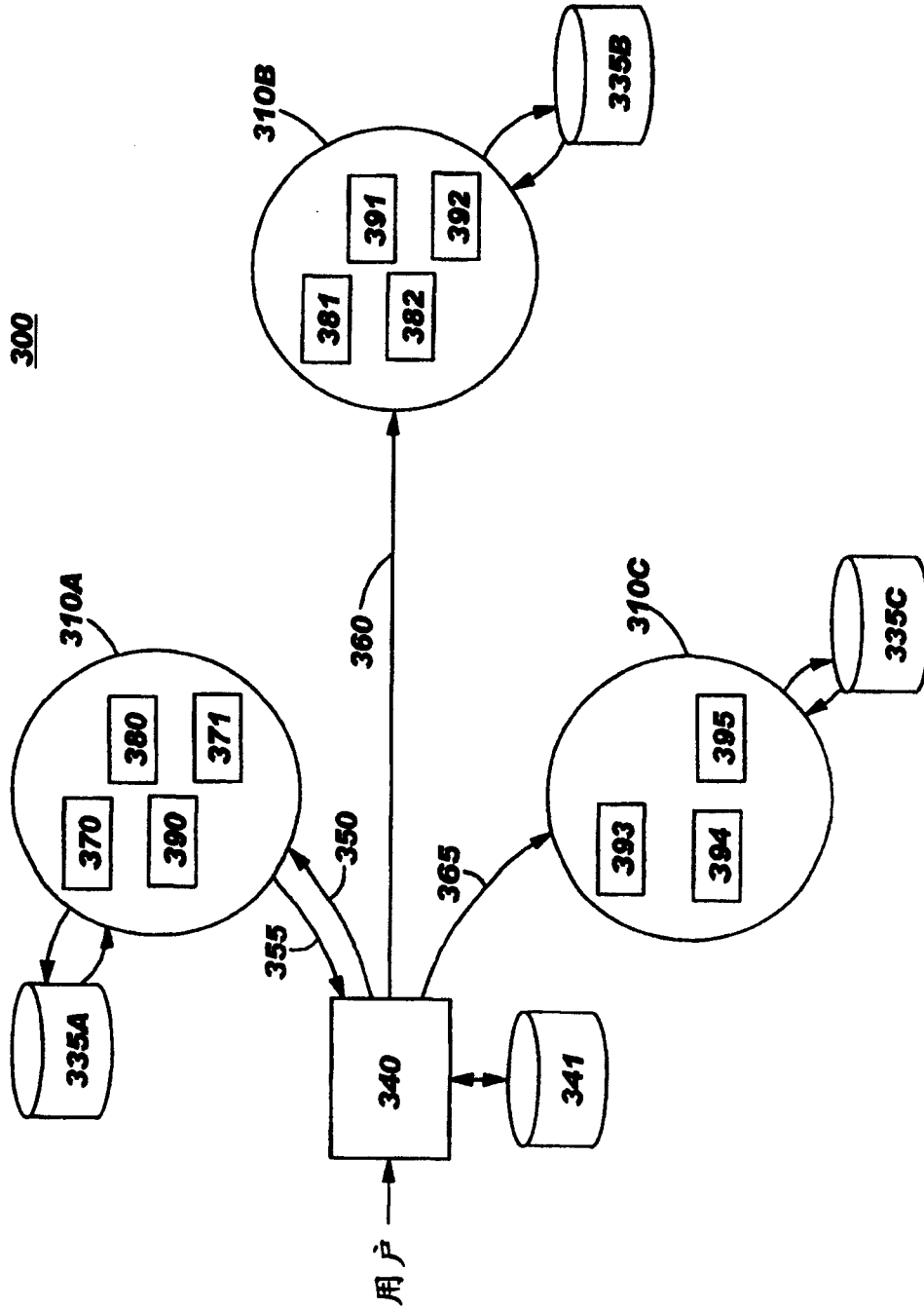


图4

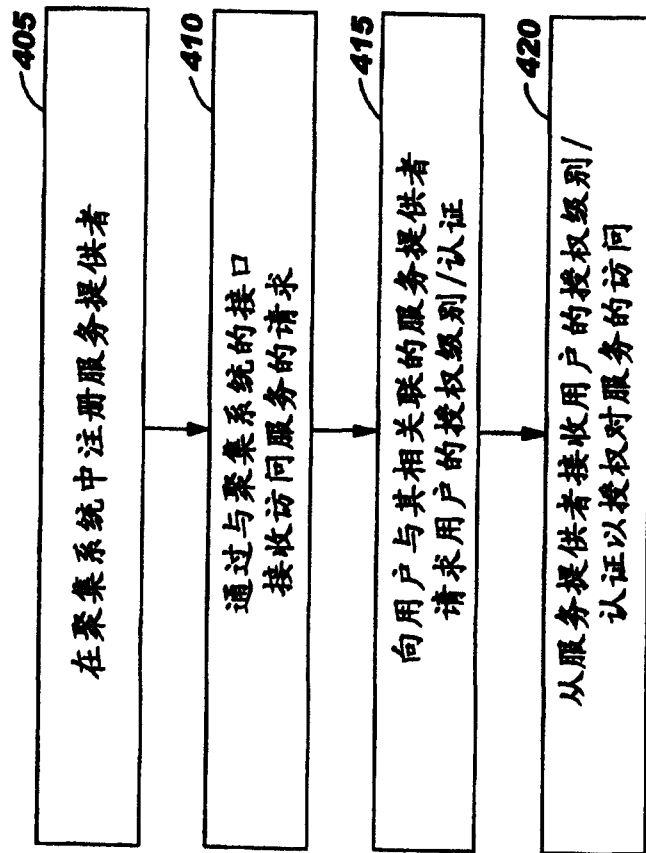


图5

用户	授权级别		
	组 1 (R)	组 2 (R)	组 3 (R)
A	1	—	—
	2	—	—
	3	—	—
B	组 1 (RW)	组 2 (R)	组 3 (R)
	1	—	—
	2	—	—
C	组 1 (RW)	组 2 (RW)	组 3 (RW)
	1	—	—
	2	—	—

