



(12) 发明专利

(10) 授权公告号 CN 102567454 B

(45) 授权公告日 2016. 04. 27

(21) 申请号 201110360021. 0

CN 101523365 A, 2009. 09. 02,

(22) 申请日 2011. 11. 15

审查员 刘宇儒

(30) 优先权数据

12/979, 117 2010. 12. 27 US

(73) 专利权人 国际商业机器公司

地址 美国纽约

(72) 发明人 S · P · 克鲁格 O · S · 派克祖尔

(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 11038

代理人 杜娟

(51) Int. Cl.

G06F 17/30(2006. 01)

(56) 对比文件

US 2010250497 A1, 2010. 09. 30,

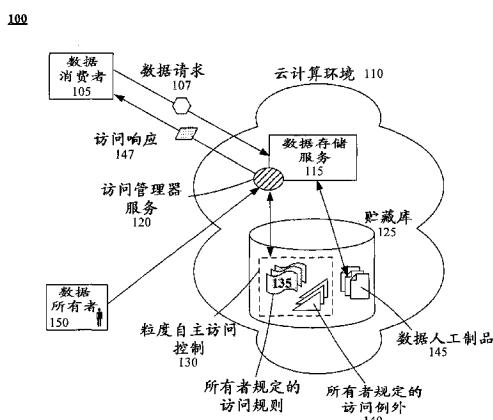
权利要求书4页 说明书11页 附图5页

(54) 发明名称

实现云计算环境中数据的粒度自主访问控制  
的方法和系统

(57) 摘要

本发明涉及实现云计算环境中数据的粒度自  
主访问控制的方法和系统。实现云计算环境中的  
自主访问控制可从通过访问管理器服务获得数据  
请求和响应消息开始。响应消息可由数据存储服  
务响应于数据请求而产生。访问管理器服务可识  
别适用于数据请求的所有者规定的访问规则和 /  
或访问例外。可通过使用适用的所有者规定的访  
问规则和 / 或访问例外确定访问响应。响应消息  
和访问响应均可表示对于请求的数据人工制品的  
访问的允许或拒绝。访问响应可与响应消息相比  
较。如果访问响应不匹配响应消息，则响应消息可  
被否决以表达访问响应。如果访问响应匹配响应  
消息，则响应消息可被传输到数据请求的发起实  
体。



1.一种计算环境中的方法,包括:

由在云计算环境中操作的访问管理器服务获得数据请求和对于数据请求的响应消息,其中,所述响应消息是由云计算环境的数据存储服务响应于数据请求而产生的,其中,所述响应消息指示对于由数据存储服务存储的数据人工制品的访问的允许和拒绝中的至少一个;

识别适用于数据请求的自主访问控制,包括:至少一个所有者规定的访问规则和至少一个所有者规定的访问例外中的至少一个的存在,所述自主访问控制能够撤销由所述数据存储服务做出的访问允许和访问拒绝;

基于识别的至少一个所有者规定的访问规则和至少一个所有者规定的访问例外确定对于数据请求的访问响应,其中,所述访问响应指示对于在数据请求中请求的数据人工制品的访问的允许和拒绝中的至少一个,其中所有者规定的访问规则定义限制访问数据人工制品的至少一个参数,并且其中所有者规定的访问例外定义允许访问数据人工制品的条件,其中访问被数据存储服务和至少一个所有者规定的访问规则中的至少一个拒绝;

比较确定的访问响应与响应消息;

如果确定的访问响应不匹配响应消息,则否决响应消息以表达确定的访问响应;和

如果确定的访问响应匹配响应消息,则将响应消息传输到数据请求的发起实体。

2.根据权利要求1的方法,其中,获得数据请求和响应消息还包含:

检测数据存储服务对数据请求的接收;和

从数据存储服务请求所述数据请求的副本。

3.根据权利要求1的方法,其中,获得数据请求和响应消息还包含:

检测数据存储服务对响应消息的传送;和

截断响应消息的传送。

4.根据权利要求1的方法,其中,如果所述识别的结果是存在所有者规定的访问例外,则所述方法还包括:

请求来自数据请求的发起实体的认证数据;

在接收到认证数据时,证实所述认证数据;和

如果认证数据被确定为有效,则立即否决响应消息以表达所有者规定的访问例外。

5.根据权利要求4的方法,还包括:

评估所有者规定的访问例外是否要保持激活以供访问管理器服务使用;和

如果所有者规定的访问例外被评估为不保持激活,则自动去激活所有者规定的访问例外,其中,所述所有者规定的访问例外不可用于访问管理器服务。

6.根据权利要求4的方法,还包括:

如果认证数据被确定为无效,则将无效认证数据通知给数据请求的发起实体;和

重复请求和证实来自发起实体的认证数据,其中,对于数据人工制品的访问被拒绝,直到有效认证数据的接收、由数据存储服务创建的与数据请求相关联的会话的终止、和预定的时间限制的期满中的至少一个。

7.根据权利要求1的方法,其中,访问响应的确定还包含:

聚合所述至少一个识别的所有者规定的访问规则;

识别所有者规定的访问规则的聚合内冲突的存在,其中,如果至少两个所有者规定的

访问规则的参数值相互排斥，则所述至少两个所有者规定的访问规则被视为冲突，

如果冲突存在，通过使用与识别为冲突的每个所有者规定的访问规则相关联的优先权值来解决所述冲突，其中，具有最高优先权值的所有者规定的访问规则优先于具有较低优先权值的所有者规定的访问规则被使用，其中从所有者规定的访问规则的聚合去除具有较低优先权值的所有者规定的访问规则；

比较与由所有者规定的访问规则的聚合表达的参数值对应的来自数据请求的数据值；

如果所述比较表示数据值满足参数值，则将访问响应设为拒绝对于数据人工制品的访问；和

如果所述比较表示参数不被数据值满足，则将访问响应设为允许对于数据人工制品的访问。

8. 根据权利要求1的方法，其中，响应消息的否决还包含：

实施对于由数据存储服务为数据请求创建的会话的至少一个参数的修改，其中，所述至少一个参数控制对会话准予的访问；

修改响应消息以反映确定的访问响应；和

将响应消息传输到数据请求的发起实体。

9. 一种计算环境中的系统，包括：

由在云计算环境中操作的访问管理器服务获得数据请求和对于数据请求的响应消息的装置，其中，所述响应消息是由云计算环境的数据存储服务响应于数据请求而产生的，其中，所述响应消息指示对于由数据存储服务存储的数据人工制品的访问的允许和拒绝中的至少一个；

识别适用于数据请求的自主访问控制，包括：至少一个所有者规定的访问规则和至少一个所有者规定的访问例外中的至少一个的存在的装置，所述自主访问控制能够撤销由所述数据存储服务做出的访问允许和访问拒绝；

基于识别的至少一个所有者规定的访问规则和至少一个所有者规定的访问例外确定对于数据请求的访问响应的装置，其中，所述访问响应指示对于在数据请求中请求的数据人工制品的访问的允许和拒绝中的至少一个，其中所有者规定的访问规则定义限制访问数据人工制品的至少一个参数，并且其中所有者规定的访问例外定义允许访问数据人工制品的条件，其中访问被数据存储服务和至少一个所有者规定的访问规则中的至少一个拒绝；

比较确定的访问响应与响应消息的装置；

如果确定的访问响应不匹配响应消息，则否决响应消息以表达确定的访问响应的装置；和

如果确定的访问响应匹配响应消息，则将响应消息传输到数据请求的发起实体的装置。

10. 根据权利要求9的系统，其中，数据存储服务进一步被配置为：

定义对于访问多个数据人工制品的限制的多个数据处理规则，其中，数据存储服务利用所述多个数据处理规则来对于请求访问数据人工制品的数据消费者确定访问允许和访问拒绝中的至少一个。

11. 根据权利要求9的系统，其中，访问管理器服务进一步被配置为：

定义限制访问数据人工制品的至少一个参数值的多个所有者规定的访问规则；和

定义允许访问数据人工制品的条件的多个所有者规定的访问例外，其中，访问被数据存储服务和至少一个所有者规定的访问规则中的至少一个拒绝。

12. 根据权利要求11的系统，其中，还包括：

被配置为证实与所有者规定的访问例外相关联的认证信息的认证机制，其中，访问管理器服务接收到有效认证数据使得能够实现访问数据人工制品。

13. 根据权利要求12的系统，其中，认证机制进一步被配置为自动产生认证信息。

14. 根据权利要求12的系统，其中，认证机制被配置为利用强认证处理。

15. 根据权利要求11的系统，还包括：

被配置为允许定义多个所有者规定的访问规则和多个所有者规定的访问例外的访问管理器服务用户界面。

16. 一种计算环境中的方法，包括：

云存储系统的数据存储服务接收数据请求，其中，所述数据请求请求访问由云计算环境内的云存储系统存储的数据人工制品；

数据存储服务确定对数据请求的响应，其中，所述确定表示对于数据人工制品允许访问和拒绝访问中的至少一个；

访问管理器服务检测数据存储服务对于数据请求的接收；

访问管理器服务在所确定的响应的执行之前中断数据存储服务对于数据请求的处理；

访问管理器服务获得数据请求的副本和数据存储服务的响应；

访问管理器服务针对为数据人工制品定义的自主访问控制来评价数据请求的副本的内容，其中，所述自主访问控制由与数据人工制品相关联的实体配置，所述自主访问控制能够撤销由所述数据存储服务做出的访问允许和访问拒绝；

访问管理器服务根据数据请求副本的所述评价确定响应，其中，所述确定表示对于数据人工制品允许访问和拒绝访问中的至少一个；

比较由数据存储服务确定的响应与由访问管理器服务在内部确定的响应；

如果所述比较表示数据存储服务和访问管理器服务的响应不一致，则访问管理器服务否决数据存储服务的响应，其中，由访问管理器服务确定的响应优先于由数据存储服务确定的响应；和

如果所述比较表示数据存储服务和访问管理器服务的响应一致，则访问管理器服务释放数据存储服务对于数据请求的处理的中断，其中，允许数据存储服务完成数据请求的实现。

17. 根据权利要求16的方法，其中，数据存储服务对于数据请求的处理的中断还包含：

访问管理器服务检测所述响应从数据存储服务向数据请求的发起实体传送；和

访问管理器服务截断所述传送。

18. 根据权利要求16的方法，其中，评价数据请求副本的内容还包含：

访问管理器服务识别适用于数据请求副本的至少一个所有者规定的访问例外的存在，其中，自主访问控制利用所有者规定的访问例外，其中所有者规定的访问例外定义允许的对数据人工制品的访问的条件，其中所述访问可被数据存储服务和自主访问控制中的至少一个拒绝；

如果至少一个适用的所有者规定的访问例外存在，则访问管理器服务请求来自数据请

求副本的发起实体的认证数据；

在接收到认证数据时，访问管理器服务证实所述认证数据；以及，

如果认证数据被确定为有效，则访问管理器服务立即否决数据存储服务的响应，其中，由访问管理器服务确定的响应优先于通过数据存储服务确定的响应。

19. 根据权利要求18的方法，其中，如果至少一个所有者规定的访问例外不存在，则所述方法还包括：

访问管理器服务识别适用于数据请求副本的至少一个所有者规定的访问规则的存在，其中，自主访问控制利用所有者规定的访问规则，其中所有者规定的访问规则定义限制访问数据人工制品的至少一个参数值；

如果至少一个适用的所有者规定的访问规则存在，则访问管理器服务聚合至少一个适用的所有者规定的访问规则；

访问管理器服务识别适用的所有者规定的访问规则的聚合内冲突的存在，其中，如果至少两个适用的所有者规定的访问规则的参数值相互排斥，则所述至少两个适用的所有者规定的访问规则被视为冲突，

如果冲突存在，访问管理器服务通过使用与被识别为冲突的每个所有者规定的访问规则相关联的优先权值来解决所述冲突，其中，具有最高优先权值的所有者规定的访问规则优先于具有较低优先权值的所有者规定的访问规则被使用，其中从适用的所有者规定的访问规则的聚合去除具有较低优先权值的所有者规定的访问规则；

访问管理器服务比较与由适用的所有者规定的访问规则的聚合表达的参数值对应的来自数据请求副本的数据值，其中，数据值满足参数值表示拒绝对于数据人工制品的访问。

20. 根据权利要求16的方法，其中，数据存储服务的响应的否决还包含：

访问管理器服务实施对于由数据存储服务为数据请求创建的会话的至少一个参数的修改，其中所述至少一个参数控制对会话准予的访问；

访问管理器服务重新启动数据存储服务对于数据请求的处理，其中，数据存储服务对数据请求的处理反映对于会话的至少一个参数的修改。

## 实现云计算环境中数据的粒度自主访问控制的方法和系统

### 技术领域

[0001] 本发明涉及云计算数据存储的领域,更具体地,涉及对于存储于云计算环境中的数据实现粒度数据所有者可配置访问控制(granular data owner-configurable access control)。

### 背景技术

[0002] 基于云的存储服务,即特别地用于数据存储和/或管理的云服务,允许组织卸载数据管理开销并且增加地理上分开的群组之间的数据可访问性。可从授权的用户能够与云存储服务连接的任何计算装置访问存储于云存储器中的数据。

[0003] 例如,修理技术人员能够从互连网连接性可用的任何作业现场访问服务手册和修理报告。

### 发明内容

[0004] 本发明的一个方面可包括用于实现云计算环境中的自主数据访问控制的方法。这种方法可开始于通过在云计算环境中操作的访问管理器服务(access manager service)获得数据请求和对于数据请求的响应消息。响应消息可以由云计算环境的数据存储服务响应于数据请求而产生。响应消息可表示对于由数据存储服务存储的数据人工制品(data artifact)的访问的允许或拒绝。可识别适用于数据请求的所有者规定的访问规则和/或所有者规定的访问例外。可基于适用的所有者规定的访问规则和/或所有者规定的访问例外确定对于数据请求的访问响应。访问响应可表示对于请求的数据人工制品的访问的允许或拒绝。所有者规定的访问规则可定义限制访问数据人工制品的参数值。所有者规定的访问例外可定义允许否则会被拒绝的对数据人工制品的访问的条件。然后,确定的访问响应可与响应消息相比较。当确定的访问响应不匹配响应消息时,响应消息可被否决 override(override)以表达(express)确定的访问响应。当确定的访问响应匹配响应消息时,响应消息可被传输到数据请求的发起实体。

[0005] 本发明的另一方面可包括能够实现对于云存储服务的自主数据访问控制的系统。这种系统可包括表示电子数据文件的数据人工制品、云计算环境、数据存储云服务和访问管理器云服务。云计算环境可包含被配置为根据云计算模型操作的云服务提供器。数据存储云服务可被配置为管理云计算环境内的数据人工制品的存储和访问。访问管理器云服务可被配置为对于由数据存储云服务管理的数据人工制品提供自主访问控制。自主访问控制可以在数据存储云服务执行的访问控制操作之外(in addition to)被执行。自主访问控制能够撤销(countermand)由数据存储云服务做出的访问允许和访问拒绝。

[0006] 本发明的另一方面可包括计算机程序产品,包含具有嵌入的计算机可用程序代码的计算机可读存储介质。计算机可用程序代码可被配置为获得数据请求和对于数据请求的响应消息。响应消息可由在云计算环境中操作的数据存储服务响应于数据请求而产生。响应消息可表示对于由数据存储服务存储的数据人工制品的访问的允许或拒绝。计算机可用

程序代码可被配置为识别适用于数据请求的所有者规定的访问规则和/或所有者规定的访问例外。然后，计算机可用程序代码可被配置为基于识别的所有者规定的访问规则和/或所有者规定的访问例外确定对于数据请求的访问响应。访问响应可表示对于请求的数据人工制品的访问的允许或拒绝。所有者规定的访问规则可定义限制访问数据人工制品的参数值。所有者规定的访问例外可定义允许否则会被拒绝的对数据人工制品的访问的条件。计算机可用程序代码可被配置为比较确定的访问响应与响应消息。当确定的访问响应不匹配响应消息时，计算机可用程序代码可被配置为否决响应消息以表达确定的访问响应。计算机可用程序代码可被配置为当确定的访问响应匹配响应消息时将响应消息传输到数据请求的发起实体。

[0007] 本发明的又一方面可包括用于实现云存储系统中的自主数据访问控制的方法。这种方法可在云存储系统的数据存储云服务接收访问由云计算环境内的云存储系统存储的数据人工制品的数据请求时开始。可通过数据存储云服务确定对于数据请求的响应，从而表示对于数据人工制品的访问的允许或拒绝。访问管理器云服务可检测数据存储云服务对于数据请求的接收。访问管理器云服务然后可在所确定的响应的执行之前中断数据存储云服务对于数据请求的处理。可通过访问管理器云服务获得数据请求的副本和数据存储云服务的响应。访问管理器云服务可针对为数据人工制品定义的自主访问控制来评价数据请求副本的内容。可通过与数据人工制品相关联的实体配置自主访问控制。可通过访问管理器云服务确定来自数据请求副本的所述评价的响应，从而表示对于数据人工制品的访问的允许或拒绝。访问管理器云服务然后可比较由数据存储云服务确定的响应与内部确定的响应。当比较表示数据存储云服务与访问管理器云服务的响应不一致时，访问管理器云服务可否决数据存储云服务的响应。当比较表示数据存储云服务与访问管理器云服务的响应一致时，访问管理器云服务可释放数据存储云服务对于数据请求的处理的中断，从而允许数据存储云服务完成数据请求的实现。

## 附图说明

[0008] 图1是示出根据这里公开的本发明的配置的实施例的通过使用云计算环境中的数据存储服务实现对于为其提供访问的数据人工制品的粒度自主访问控制的概念处理流程图。

[0009] 图2是示出根据这里公开的本发明的配置的实施例的对于在云计算环境中操作的数据存储服务提供粒度自主访问控制的系统的示意图。

[0010] 图3是在总体上详述根据这里公开的本发明的配置的实施例的用于实现自主访问控制的关于数据存储服务的访问管理器服务的功能的方法的流程图。

[0011] 图4是描述根据这里公开的本发明的配置的实施例的访问管理器服务的操作的方法的流程图。

[0012] 图5是详述根据这里公开的本发明的配置的实施例的数据所有者对访问管理器服务使用的方法的流程图的集合。

## 具体实施方式

[0013] 虽然数据存储和数据传送总是关心数据安全性，但是，控制其它用户和/或组织对

于存储的数据的访问或可见性对于数据所有者(即,授权用户、组织)来说经常是受限的。由于云服务一般被设计为适应广泛的用户类型和需求,因此,云服务的特征和/或能力本质上常常是基本的或一般性的。因而,当与许多组织所习惯的企业级数据管理系统相比时,可用于云存储服务中的访问控制的类型(即,访问控制列表、用户群组、基于角色的访问等)是相对简单的。

[0014] 利用云存储服务的每个组织被限于相同的访问控制。虽然基于角色的访问控制方法可以适用于大的组织,但它对于较小的组织可能过度复杂。类似地,适于中小组织的基于用户群组的方法对于大企业可能是不适用的。

[0015] 并且,一个组织的通过云存储服务存储的数据受到服务提供器的可见性和/或访问规则的约束。在云存储服务提供器改变它们的可见性/访问规则的情况下,对于组织的数据的访问可能会受损。

[0016] 本发明公开了一种用于实现对于由云计算环境中的数据存储云服务处理的数据人工制品的自主数据访问控制的方案。数据存储云服务可管理数据人工制品的存储和访问。访问管理器云服务可应用一组自主访问控制,以动态调整由数据存储云服务确定的对于数据人工制品的访问的允许或拒绝。自主访问控制可由所有者规定的访问规则和所有者规定的访问例外表示。所有者规定的访问规则可定义限制对于数据人工制品的访问的参数值。所有者规定的访问例外可定义允许否则会被拒绝的对数据人工制品的访问的条件。

[0017] 本领域技术人员可以理解,本发明的方面可实现为系统、方法或计算机程序产品。因此,本发明的方面可采取完全硬件实施例、完全软件实施例(包含固件、驻留软件、微代码等)或组合软件和硬件方面的实施例,它们在这里均可被统称为“电路”、“模块”或“系统”。并且,本发明的方面可采取实施在具有在其上面实施的计算机可读程序代码的一个或更多个计算机可读介质中的计算机程序产品的形式。

[0018] 可以利用一个或更多个计算机可读介质的任意组合。计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质可例如为但不限于电子、磁、光学、电磁、红外或半导体系统、装置或设备或以上的任意适当的组合。计算机可读存储介质的更具体的例子(非详尽的列表)会包含以下方面:具有一个或更多个导线的电连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦可编程只读存储器(EPROM或闪存)、光纤、便携式光盘只读存储器(CD-ROM)、光学存储设备、磁存储设备或以上的任意适当的组合。在本文件的上下文中,计算机可读存储介质可以是可包含或存储供指令执行系统、装置或设备使用或与其组合的程序的任何有形介质。

[0019] 计算机可读信号介质可例如在基带中或作为载波的一部分包含具有在其中实施的计算机可读程序代码的传播的数据信号。这种传播的信号可采取包含但不限于电磁、光学或它们的任意适当的组合的各种形式中的任一种。计算机可读信号介质可以为不是计算机可读存储介质并且可传送、传播或传输供指令执行系统、装置或设备使用或与其组合的程序的任何计算机可读介质。

[0020] 可通过使用包含但不限于无线、有线、光纤电缆、RF等或以上的任意适当的组合的任意适当的介质传送在计算机可读介质上实施的程序代码。可以包括诸如Java、Smalltalk、C++等的面向对象的编程语言和诸如“C”编程语言或类似的编程语言的常规的过程编程语言的一个或更多个编程语言的任意组合编写用于实施本发明的方面的操作的

计算机程序代码。程序代码可完全在用户的计算机上、部分地在用户的计算机上、作为独立软件包、部分地在用户的计算机上并且部分地在远程计算机上、或者完全在远程计算机或服务器上执行。在后一种方案中，远程计算机可通过包含局域网络(LAN)或广域网络(WAN)的任意类型的网络与用户的计算机连接，或者，可与外部计算机连接(例如，使用互连网服务提供商通过互连网)。

[0021] 以下参照根据本发明的实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明的方面。可以理解，可通过计算机程序指令实现流程图和/或框图的各块和流程图和/或框图中的块的组合。这些计算机程序指令可被提供给通用计算机、专用计算机或其它的可编程数据处理装置的处理器，以生成机器，使得通过计算机或其它的可编程数据处理装置的处理器执行的指令产生用于实现在流程图和/或框图块中规定的功能/动作的装置。

[0022] 这些计算机程序指令也可被存储于计算机可读介质中，该计算机可读介质可引导计算机、其它的可编程数据处理装置或其它的设备以以特定的方式工作，使得存储于计算机可读介质中的指令产生包含实现在流程图和/或框图块中规定的功能/动作的指令的制造物品。

[0023] 计算机程序指令也可被加载到计算机、其它的可编程数据处理装置或其它的设备上，以导致在计算机、其它的可编程装置或其它的设备上执行一系列的操作步骤，以产生计算机实现的处理，使得在计算机或其它的可编程装置上执行的指令提供用于实现在流程图和/或框图块中规定的功能/动作的处理。

[0024] 图1是示出根据这里公开的本发明的配置的实施例的通过使用云计算环境110中的数据存储服务115实现对于对其提供访问的数据人工制品145的粒度自主访问控制130的概念处理流程图100。

[0025] 在处理流程100中，数据消费者105可向在云计算环境110中操作的数据存储服务115发送对于数据人工制品145的数据请求107。数据消费者105可与请求访问指定的数据人工制品145的人类用户和/或计算实体对应。数据人工制品145可表示以电子格式中存储的各种数据(即，文本文件、图像文件、音频文件、多媒体文件等)。

[0026] 数据请求107可以是识别提出请求的数据消费者105和要被访问的数据人工制品145的电子消息。根据消息格式和/或数据存储服务115，数据请求107还可包含各种其它消息传递信息，诸如提出请求的数据消费者105的互连网协议(IP)地址、由数据消费者105执行的动作和数据请求107的时间戳等。

[0027] 云计算环境110可表示根据云计算模型配置的硬件/软件计算环境。云计算环境110可实现对于像贮藏库(repository)125那样的可配置计算资源的共享池的按需访问。云计算环境110可实现为私有云(即，由单独的组织所有)、社区云(即，由多个和谐的组织共享)、公共云(即，可用于公众或大群组)或混合云(即，多个云类型的配置)。

[0028] 数据存储服务115可表示特别地被配置为管理其相关联的云贮藏库125中的数据人工制品145的存储和访问的云服务。数据存储服务115和贮藏库125可表示统称为云存储系统或云存储服务的东西。除了数据人工制品145的简单的存储，数据存储服务115也可包含诸如文件共享、版本控制和在线协作的各种数据管理功能。

[0029] 数据存储服务115可确定是允许还是拒绝数据请求107。但是，与典型的数据存储

服务115实现中不同,访问管理器服务120可中断由数据存储服务115对于数据人工制品145的提供,以基于粒度自主访问控制130(这里称为自主访问控制130)检查是否允许数据人工制品145的提供。

[0030] 访问管理器服务120可表示被配置为用作实现在由数据存储服务115提供的数据人工制品145上执行自主访问控制130的独立机制的云服务。即,访问管理器服务120可基于在自主访问控制130中定义的参数来调整数据存储服务115向数据消费者105的数据人工制品145的提供。

[0031] 例如,自主访问控制130可被用来将对于特定的数据人工制品145的访问限制到仅三个用户105,即使数据存储服务115通常会向其它的用户105提供数据人工制品145。

[0032] 自主访问控制130可表示可根据数据人工制品145的数据所有者150的裁量被设定以允许和/或拒绝对于数据人工制品145的访问的可配置参数。数据所有者150可表示数据人工制品145的授权用户或组织或具有授权以代表授权用户/组织的用户。

[0033] 例如,授权组织的数据管理员可被给予管理对于所有数据人工制品145的自主访问控制130的任务,尽管不是数据人工制品145的授权用户。

[0034] 自主访问控制130可包含所有者规定的访问规则135和所有者规定的访问例外140。所有者规定的访问规则135(这里称为访问规则135)可表示限制对于数据人工制品145的访问的条件。所有者规定的访问例外140(这里称为访问例外140)可表达对于访问规则135的经授权的例外。访问规则135可意味着标准策略,而访问例外140可表示与标准策略相反的偶然和/或暂时的允许。

[0035] 用于访问规则135和访问例外140的参数可利用在数据请求107内包含的数据字段、对于数据人工制品145定义的元数据和/或由数据存储服务115利用的数据要素(例如,用户名称、用户角色、访问等级等)。

[0036] 一旦访问管理器服务120查明数据请求107是否应被允许/拒绝,访问管理器服务120可确定通过数据存储服务115的数据人工制品145的提供应该被否决还是继续。根据该确定,访问管理器服务120可向数据消费者105发送适当的访问响应147(即,访问准予/拒绝)。

[0037] 为了示出常规的方法和由自主访问控制130提供的方法之间的差异,使用外部实体105需要一次访问以查看一般限于内部用户105的数据人工制品145的例子。

[0038] 当使用常规的云数据存储服务115时,通过使用数据存储服务115的可用的访问控制机制,外部实体105可被分配对于数据人工制品145的适当访问等级(即,向外部实体105分配适当的角色)。但是,这样做将向外部实体105提供对于可用于该访问等级的所有数据人工制品145的不受限的访问-如果其它的敏感内部数据人工制品145共享该访问等级,那么这是不希望的情况。

[0039] 作为替代,我们尝试通过使用只能访问特定的数据人工制品145的数据存储服务115的访问控制机制来定义新的角色/群组。虽然是更好的选择,但是,访问控制机制很可能在广义上被定义并且将不支持对于外部实体105能够在数据人工制品145上执行的动作类型的限制。因此,该方法虽然将外部实体105的访问限于特定的数据人工制品145,但不能确保外部实体105将只能查看数据人工制品145。

[0040] 对于这两个选择,数据所有者150必须记着一旦确定访问会话完成则从数据存储

服务115的访问控制机制去除或去激活(deactivate)外部实体105的访问。

[0041] 另一常用的用于处理这种情况的手段可以是以电子的方式向外部实体105提供数据人工制品145的副本(即,电子邮件、文件传送)。在这种情况下,数据所有者150放弃对于数据人工制品145的控制;外部实体105可以没有限制地分配和/或修改数据人工制品145。如果外部实体105对数据人工制品145处理不当,那么该选择会有损于组织。

[0042] 作为替代方案,可对于数据存储服务115使用UNIX或类UNIX操作系统的固有文件安全特征。UNIX或类UNIX操作系统可使保护位与存储的数据人工制品145相关联,保护位对于数据所有者、所有者属于的群组和所有其它的用户定义读取/写入/执行许可。虽然该特征顾及外部实体105可关于数据人工制品145执行的动作,但是,该选择会招致与访问有关的其它问题。

[0043] 首先,大多数的组织利用基于INTEL的操作系统,这在通过不同的操作系统尝试存储数据人工制品145时可导致互操作性问题。第二,只能通过实际的作者(创建数据人工制品145的用户)或系统管理员执行改变保护位以改变许可。由于这是基于云的数据存储服务115,因此,可能不能向数据所有者150提供任何执行基于操作系统的命令的能力。

[0044] 即使这些问题被克服,该方法也可能具有其它的与性能有关的缺点。不能使用保护位来支持其中数据消费者105和/或数据所有者150可能是多个群组的成员的访问控制机制。并且,数据消费者105属于的群组不能与要被赋予群组许可的数据所有者150不同。不能使用系统管理员以外的代理来做出许可改变。最后,一旦保护位改变,该改变就可能没有区别地影响群组的所有成员的访问。

[0045] 通过使用访问管理器服务120,将数据人工制品145限于内部用户可被表示为访问规则135,因为它是这个和/或其它数据人工制品145的标准访问策略。外部实体105访问数据人工制品145的需要可被定义为访问例外140。访问例外140可被编写为对于外部实体105的标识符是特有的,将允许的动作仅限于查看并且仅允许单个访问会话。

[0046] 并且,通过该方法,数据人工制品145可保持安全地存储于贮藏库125中;外部实体105不能存储本地副本。由访问规则135表示的数据人工制品145的标准访问策略可保持完整。一旦访问管理器服务120执行了访问例外140,访问例外140可被去激活以防止外部实体105对于数据人工制品145的进一步访问。

[0047] 通过该方法,可以在云计算环境110中提供以下的能力:

[0048] • 基于组织的操作国的数据访问规定/限制的组织特有的“拒绝方列表”,而不管贮藏库125驻留在什么国家,

[0049] • 如果数据存储服务115被损害和/或改变它们的内部访问/可见性规则,数据泄漏的最小化

[0050] • 云数据存储服务115主持(host)组织的内联网的能力

[0051] 云计算环境110可包含传输在载波内编码的数据所需要的任何硬件/软件/和固件。数据可包含于模拟或数字信号内并且通过数据或语音信道被传输。云计算环境110可包含本地组件和在计算设备组件间以及在集成设备组件和外围设备之间交换通信所需要的数据路径。云计算环境110还可包含一起形成例如互连网的数据网络的网络设备,诸如路由器、数据线、集线器和中间服务器。云计算环境110还可包含诸如电话交换机、调制解调器、蜂窝式通信塔等的基于电路的通信组件和移动通信组件。云计算环境110可包含基于线路

的和/或无线通信路径。

[0052] 如这里使用的那样,给出的贮藏库125可以是被配置为存储数字信息的物理或虚拟存储空间。可以在物理上在包含但不限于磁盘、光盘、半导体存储器、数字编码塑料存储器、全息存储器或任何其它的记录介质的任意类型的硬件内实现贮藏库125。贮藏库125可以是独立存储单元以及由多个物理设备形成的存储单元。另外,可以以各种方式在贮藏库125内存储信息。例如,可以在数据库结构内或者可以在文件存储系统的一个或更多个文件内存储信息,这里,每个文件可以出于信息搜索目的而被索引或者可以不被索引。并且,贮藏库125可利用一个或更多个加密机制以保护存储的信息以避免未授权的访问。

[0053] 图2是示出根据这里公开的本发明的配置的实施例的对于在云计算环境205中操作的数据存储服务225提供粒度自主访问控制的系统200的示意图。可以在处理流程100的上下文中利用系统200。

[0054] 在系统200中,可通过数据存储服务225在云计算环境205的贮藏库210内存储数据人工制品215。数据人工制品215的数据所有者280可利用访问管理器服务245的所有者规定的访问规则255(这里称为访问规则255)和/或所有者规定的访问例外260(这里被称为访问例外260),来为寻求对于数据人工制品215的访问的数据消费者265定义自主访问控制。

[0055] 数据所有者280可表示数据人工制品215的授权用户或发起组织或具有代表授权用户/组织的授权的用户。数据消费者265可与请求访问指定的数据人工制品215的人类用户和/或计算实体(即,其它的云服务)对应。数据人工制品215可表示以电子格式存储的各种数据(即,文本文件、图像文件、音频文件、多媒体文件等)。

[0056] 云计算环境205可表示实现云计算模型的硬件/软件组件的配置。一般地,云计算环境205可包含诸如服务器、数据存储装置和软件应用的支持在互连网上提供云服务的硬件/软件组件。

[0057] 在本例子中,云计算环境205可包含用于数据人工制品215的存储的贮藏库210、用于数据存储服务225的服务提供器(service provider)220和用于访问管理器服务245的服务提供器240。

[0058] 应当注意,在不背离本公开的本实施例的精神的情况下,附加的贮藏库210和/或服务提供器220和/或240以及由服务提供器220和/或240提供的其它的云服务可包含于云计算环境205内。

[0059] 注意,同样重要的是,由于云计算环境205基于互连网,因此,系统200的各种组件之间的通信所需要的任何计算机网络(例如,公有、私有、WAN、LAN等)可作为云计算环境205的一部分被包含并且未作为单独的实体被示出。

[0060] 服务提供器220和240可表示支持它们各自的服务225和245的操作所需要的硬件和/或软件组件。在另一设想的实施例中,数据存储服务225和访问管理器服务245可由同一服务提供器220或240提供。

[0061] 在系统200中,每个服务提供器220和240可被示为分别具有单独的数据存储装置230和250。应当注意,数据存储装置230和250的使用是要示出每个云服务225和245特定的数据要素的逻辑分离,而不旨在表达所需的实现。在系统200的实现中,数据存储装置230和/或250的内容可被存储于贮藏库210和/或可通过相应的服务提供器220或240访问的另一种贮藏库210中。即,数据存储装置230和250的内容可存储于包含在云计算环境205中

的可由服务提供器220或240访问的任何贮藏库210上。

[0062] 数据存储服务225可表示被配置为管理云贮藏库210中的数据人工制品215的存储和访问的云服务。除了数据人工制品215的存储以外,数据存储服务225还可包含诸如文件共享、版本控制和在线协作的各种数据管理功能。

[0063] 数据存储服务225可基于数据存储服务225特定的一组数据处理规则(data handling rule)235来确定是允许还是拒绝对于数据人工制品215的访问。数据处理规则235可表示由政府机构或组织施加的适用于服务提供器220、贮藏库210、数据所有者280和/或数据消费者265的位置的数据访问要求和/或规定。

[0064] 例如,对基于美国的医疗数据的数据存储服务225可具有确保由数据存储服务225处理的数据人工制品215符合健康保险携带和责任法案(HIPAA)的数据处理规则235。

[0065] 访问管理器服务245可表示被配置为用作独立机制的云服务,该独立机制可根据数据所有者280的裁量对于由数据存储服务225提供的数据人工制品215通过访问规则255进一步限制访问或者通过访问例外260允许特许。访问管理器服务245因此能够在提供对于受访问规则255和/或访问例外260约束的数据人工制品215的访问时否决数据存储服务225的决定。

[0066] 如上所述,访问规则255可意味着标准策略的表示,而访问例外260可表示对由数据存储服务225的数据处理规则235和/或访问管理器服务245的访问规则255体现的策略的偶然和/或暂时的免除。

[0067] 应当强调,访问规则255和访问例外260的管理和执行独立于数据存储服务225的操作而发生。即,访问管理器服务255可在数据存储服务225完成其操作之后执行其操作。数据存储服务225可以在不知道访问管理器服务255的动作的情况下操作。因此,访问管理器服务255的功能可被应用于当前的数据存储服务225,而不需要云计算环境205内的体系和/或系统变化。

[0068] 在另一实施例中,可在提供对所请求的数据人工制品215的访问之前作为访问控制的最终阶段由数据存储服务225调用访问管理器服务255。

[0069] 用于表达访问规则255和访问例外260的参数可利用包含于由数据存储服务225从数据消费者265接收的数据请求内的数据字段、对于数据人工制品215定义的元数据和/或由数据存储服务225利用的数据要素。

[0070] 这些参数的例子可包含但不限于用户名称、电子邮件地址、电子邮件域、IP地址、数据人工制品215的类型、用户角色、执行的动作的类型、数据人工制品215的置信度水平、接收请求的时间和请求路由等。

[0071] 数据所有者280可通过使用在客户机装置270上运行的访问管理器用户界面275定义访问规则255和/或访问例外260。客户机装置270可表示能够运行访问管理器用户界面275并与云计算环境205通信的各种计算装置。

[0072] 访问管理器用户界面275可表示其中可向数据所有者280呈现用于定义访问规则255和/或访问例外260的可配置机制的图形用户界面(GUI)。访问管理器用户界面275可进一步被配置为利用安全措施来限制对于数据项和/或特征的访问或使用。

[0073] 例如,为了将访问例外260的创建限制于具有“管理员”角色的数据所有者280,可以使用基于角色的方法。并且,可以使用不同的角色来限制数据所有者280可创建和/或修

改的访问规则255的类型。

[0074] 应当注意,不使用访问管理器用户界面275来与数据存储服务225交互作用。与数据存储服务225的交互作用将利用与数据存储服务225相关联的用户界面(未示出)。

[0075] 云计算环境205可包含传输在载波内编码的数据所需要的任何硬件/软件/和固件。数据可包含于模拟或数字信号内并且通过数据或语音信道被传输。云计算环境205可包含本地组件和在计算设备组件间以及在集成设备组件和外围设备之间交换通信所需要的数据路径。云计算环境205还可包含一起形成例如互连网的数据网络的网络设备,诸如路由器、数据线、集线器和中间服务器。云计算环境110还可包含诸如电话交换机、调制解调器、蜂窝式通信塔等的基于电路的通信组件和移动通信组件。云计算环境205可包含基于线路的和/或无线通信路径。

[0076] 如这里使用的那样,给出的贮藏库210和数据存储装置230和250可以是被配置为存储数字信息的物理或虚拟存储空间。可以在物理上在包含但不限于磁盘、光盘、半导体存储器、数字编码塑料存储器、全息存储器或任何其它的记录介质的任意类型的硬件内实现贮藏库210和数据存储装置230和250。贮藏库210和数据存储装置230和250可以是独立存储单元以及由多个物理设备形成的存储单元。另外,可以以各种方式在贮藏库210和数据存储装置230和250内存储信息。例如,可以在数据库结构内或者可以在文件存储系统的一个或更多个文件内存储信息,这里,每个文件可以出于信息搜索目的而被索引或者可以不被索引。并且,贮藏库210和/或数据存储装置230和/或250可利用一个或更多个加密机制来保护存储的信息以避免未授权的访问。

[0077] 图3是在总体上详述根据这里公开的本发明的配置的实施例的用于实现自主访问控制的关于数据存储服务的访问管理器服务的功能的方法300的流程图。可以在处理流程100和/或系统200的上下文内执行方法300。

[0078] 方法300可示出由数据存储服务执行的一系列步骤305~325和响应于数据存储服务执行步骤305和325而被触发的由访问管理器服务执行的第二组步骤350~395。为了简化,首先讨论方法300的与数据存储服务有关的一部分,然后讨论访问管理器服务的那些步骤。

[0079] 方法300的步骤305~325可表示由数据存储服务对数据请求的典型的处理。在步骤305中,数据存储服务可从数据消费者接收数据请求。如果需要的话,在步骤310中,数据存储服务可启动用于数据消费者的用户会话。

[0080] 在步骤315中,数据存储服务可基于其内部处理规则确定对于数据请求的提供器响应(即,允许,拒绝)。应当注意,使用术语“提供器响应”来区分由数据存储服务确定的响应和由访问管理器服务确定的响应(由术语“访问响应”表示)。

[0081] 数据存储服务然后可在步骤320中创建对于数据请求的响应消息。在步骤325中,可通过数据存储服务向请求者(数据消费者)发送响应消息。

[0082] 如虚线307所示,数据存储服务执行步骤305可触发访问管理器服务执行步骤350。在步骤350中,访问管理器服务可诸如通过使用监听器部件或通过询问数据存储服务的消息队列来检测数据存储服务已接收数据请求。

[0083] 在步骤355中,访问管理器服务可获得数据请求的副本。在步骤360中,访问管理器服务可识别适用于数据请求的所有者规定的访问规则和/或例外。然后,在步骤365中,可由

访问管理器服务基于识别的访问规则和/或例外确定对于数据请求的访问响应。

[0084] 访问管理器服务可响应于数据存储服务执行步骤325而执行步骤370。在步骤370中,访问管理器服务可截断(intercept)数据存储服务发送的响应消息。访问管理器服务可在步骤375中确定它确定的访问响应是否匹配截断的响应消息的提供器响应。

[0085] 当响应匹配(即,两个服务均同意请求者应具有或不应具有访问权)时,可以执行步骤380,其中访问管理器服务向请求者发送响应消息(即,释放截断的响应消息)。

[0086] 当响应不匹配时,访问管理器服务可在步骤385中否决数据存储服务的响应消息。在执行步骤385的点上,可存在两种可能的情况-访问管理器服务希望拒绝数据存储服务允许的访问或允许数据存储服务拒绝的访问。

[0087] 在任一种情况下,可以执行步骤390,其中访问管理器服务可向数据存储服务提供对于请求者的会话许可的必要的否决修改。访问管理器服务然后可在步骤395中修改响应消息的响应并且将响应消息发送给请求者。

[0088] 图4是描述根据这里公开的本发明的配置的实施例的访问管理器服务的操作的方法400的流程图。可以在处理流程100、系统200的上下文内和/或与方法300结合执行方法400。

[0089] 方法400可在步骤405开始,其中访问管理器服务可获得数据请求和由数据存储服务确定的响应消息。可在步骤410中对于数据请求识别所有者规定的访问规则和/或例外。

[0090] 在步骤415中,可以确定对于数据请求是否存在访问例外。当不存在访问例外时,识别的访问规则可在步骤420中聚合(aggregate)。

[0091] 由于访问规则可能由单独的用户产生、在各种粒度水平上存在并且/或者适用于不同参数,因此,存在访问规则相互冲突的可能性。访问管理器服务可利用优先权值以确立哪个访问规则应占先。如果需要的话,可以在步骤425中使用该优先权值以解决识别的访问规则之间的冲突。

[0092] 在步骤430中,可基于识别的访问规则确定访问响应。可以在步骤435中确定所确定的访问响应是否匹配来自数据存储服务的响应消息。

[0093] 当确定的访问响应匹配响应消息时,可以执行步骤440,其中将响应消息传输到请求者(数据消费者)。当确定的访问响应不匹配响应消息时,在步骤465中,请求者的会话可被修改以按每个确定的访问响应允许或拒绝访问。在步骤470中,反映确定的访问响应的响应消息可被发送给请求者。

[0094] 当在步骤415中确定存在访问例外时,方法400的流程可前进到步骤445,其中访问管理器服务可请求来自请求者的请求认证。对于访问例外的认证可以是附加的安全阶段,并可被推荐用于敏感或专用数据人工制品。

[0095] 认证可采取各种形式,包含但不限于质询/响应格式、一次性密码、数字令牌、存储于智能卡上的认证参数、管理员对会话的人工授权、生物测定读数、认证形式的组合等。

[0096] 可在步骤450中确定认证的有效性。当请求者提供有效的认证时,可执行步骤455,其中访问管理器服务可根据访问例外修改请求者的会话。

[0097] 当请求者提供无效的认证时,可在步骤460中将无效的认证通知给请求者。从步骤460,流程可返回再次请求认证的步骤445。

[0098] 图5是详述根据这里公开的本发明的配置的实施例的数据所有者使用访问管理器

服务的方法500和520的流程图的集合。可以在处理流程100、系统200的上下文内和/或与方法300和/或400结合执行方法500和/或520。

[0099] 在方法500中,用户可在步骤505中通过使用访问管理器用户界面定义新的访问规则。然后可在步骤510中向输入的访问规则分配优先权值。

[0100] 作为替代方案,访问管理器服务可被配置为自动执行步骤510,从而基于创建访问规则的用户分配优先权值。例如,与由团队级用户创建的访问规则相比,由管理员级用户创建的访问规则可被自动分配更高的优先权值。

[0101] 在步骤515中,可存储新的访问规则供访问管理器服务使用。

[0102] 方法520可描述访问例外的创建。方法520可在步骤525中开始,其中管理员可在访问管理器用户界面中定义访问例外。可以在步骤530中确定是否启用自动认证(即,由访问管理器服务自动产生的认证信息)。

[0103] 由访问管理器服务使用的自动认证的类型可被扩展为包含强认证,即需要两种或更多种识别手段的认证方法。例如,访问管理器服务可产生暂时的密码和质询/响应组。为了获得访问,请求者必须正确地输入密码和响应。

[0104] 当自动认证被启用时,访问管理器服务可在步骤535中向管理员提供认证信息。在步骤540中,管理器可向准予访问的指定用户提供认证信息。从步骤540,如方法400的步骤445和450那样,访问管理器服务可继续以电子的方式认证指定的用户。

[0105] 当自动认证不被启用时,可执行步骤545,其中管理员可等待指定用户的带外认证。例如,指定的用户可联系管理员并且在口头上提供识别信息(即,地址、出生日期、社会安全号码)。

[0106] 可以在步骤550中确定有效认证的接收。当接收的认证有效时,管理员可在步骤555中为访问管理器服务手动激活访问例外。当接收的认证无效时,方法520的流程可返回步骤545,其中管理员可继续等待有效的认证。

[0107] 图中的流程和框图示出根据本发明的各种实施例的系统、方法和计算机程序产品的可能的实现的结构、功能和操作。在这方面,流程图或框图中的各块可表示包含用于实现规定的逻辑功能的一个或更多个可执行指令的模块、段或代码的一部分。应当注意,在一些替代性实现中,在块中注明的功能的次序可以与在图中注明的次序不同。例如,根据包含的功能,连续示出的两个块事实上可被基本上同时执行,或者,各块有时可以以相反的次序被执行。还应注意,可通过执行规定的功能或动作的基于专用硬件的系统或专用硬件和计算机指令的组合,实现框图和/或流程图的每个块和框图和/或流程图的各块的组合。

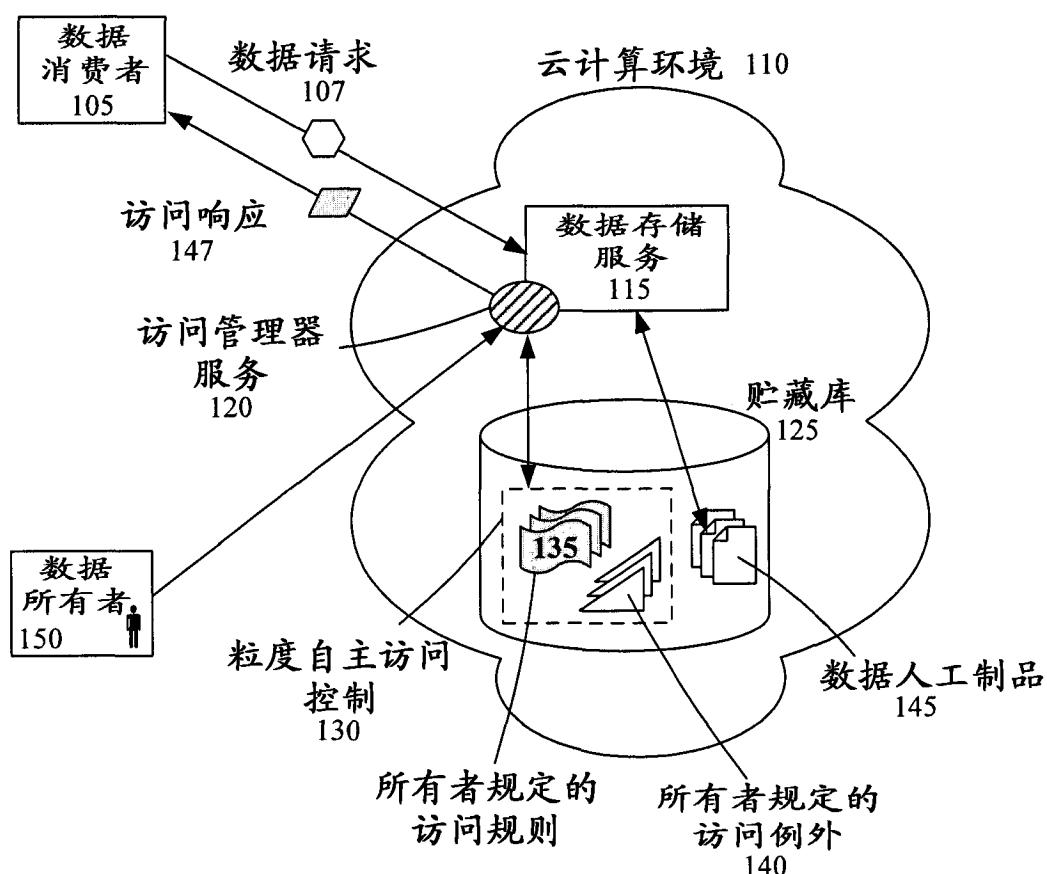
**100**

图1

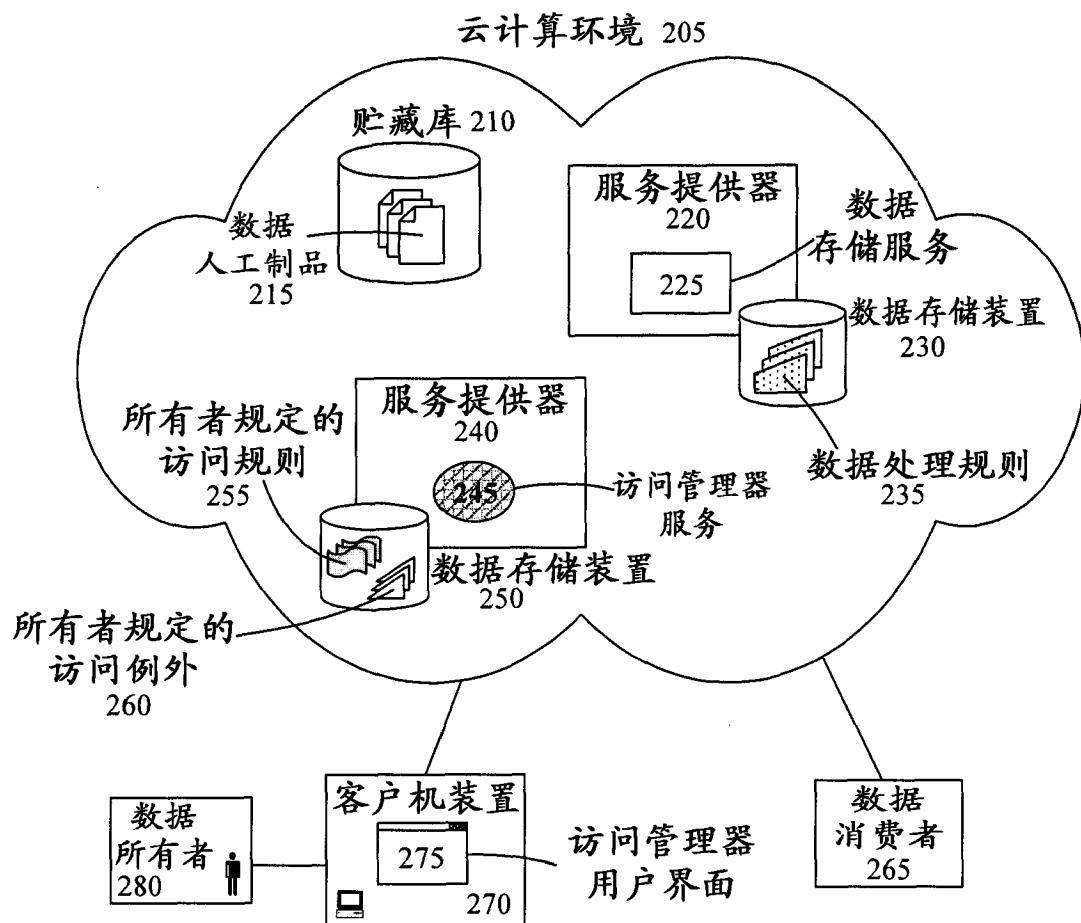
200

图2

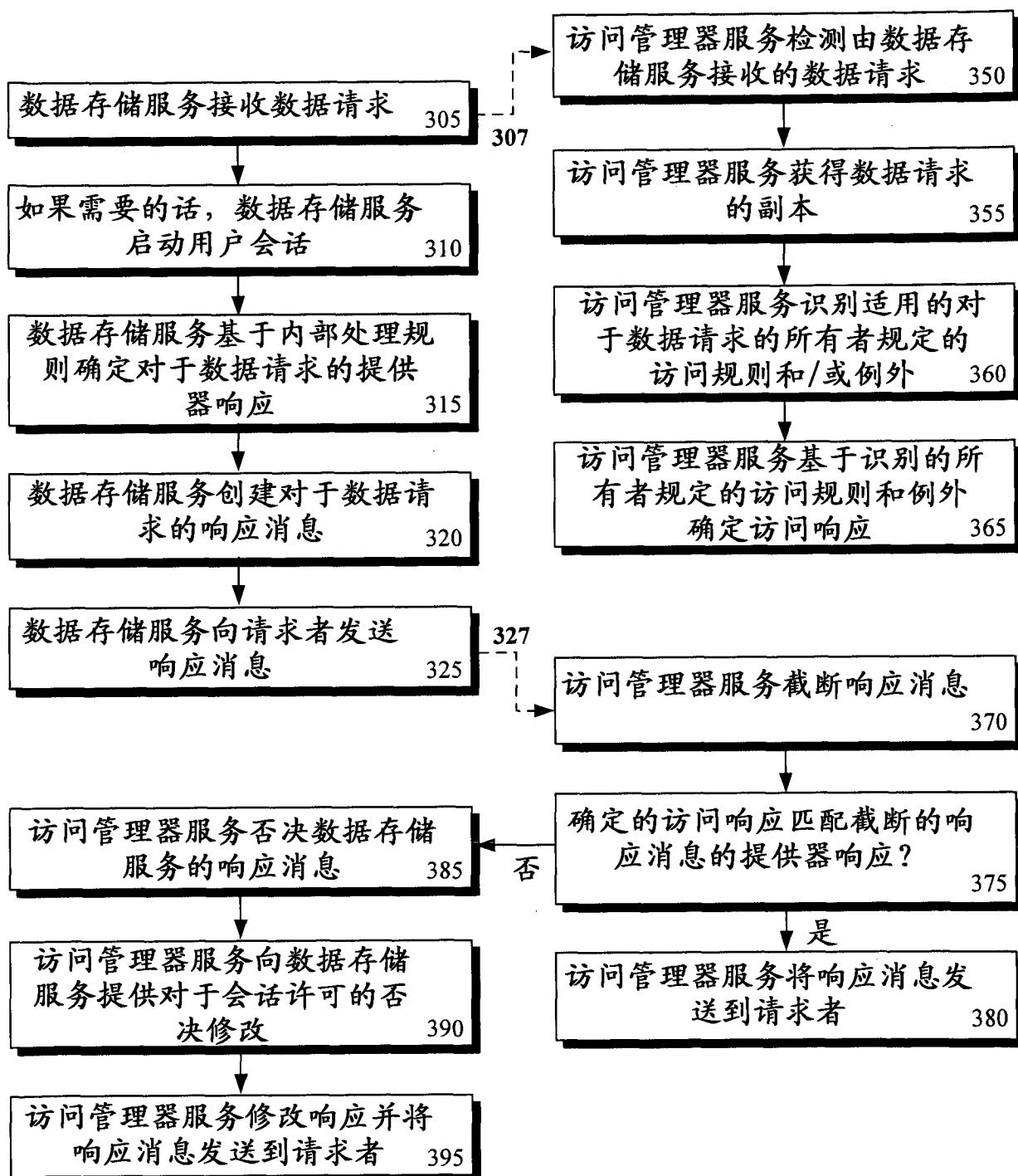
300

图3

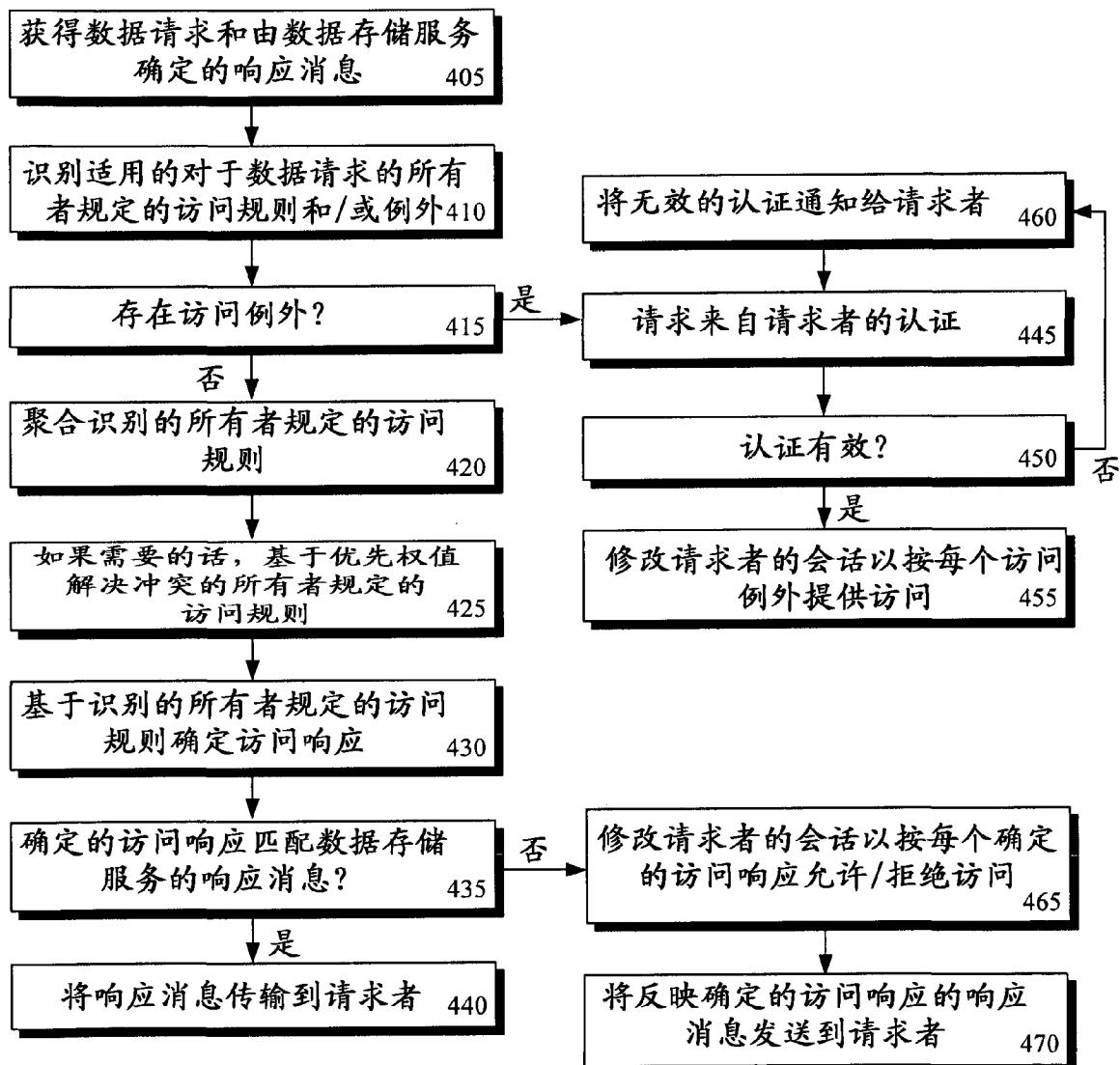
400

图4

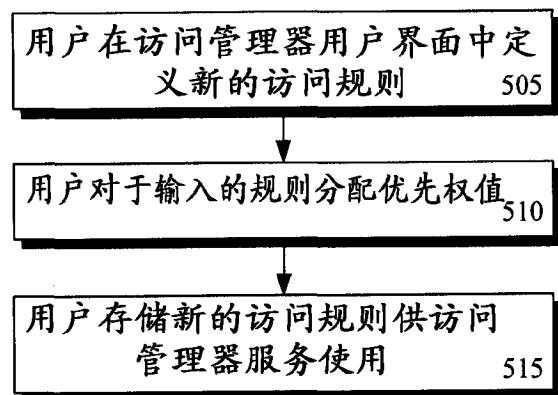
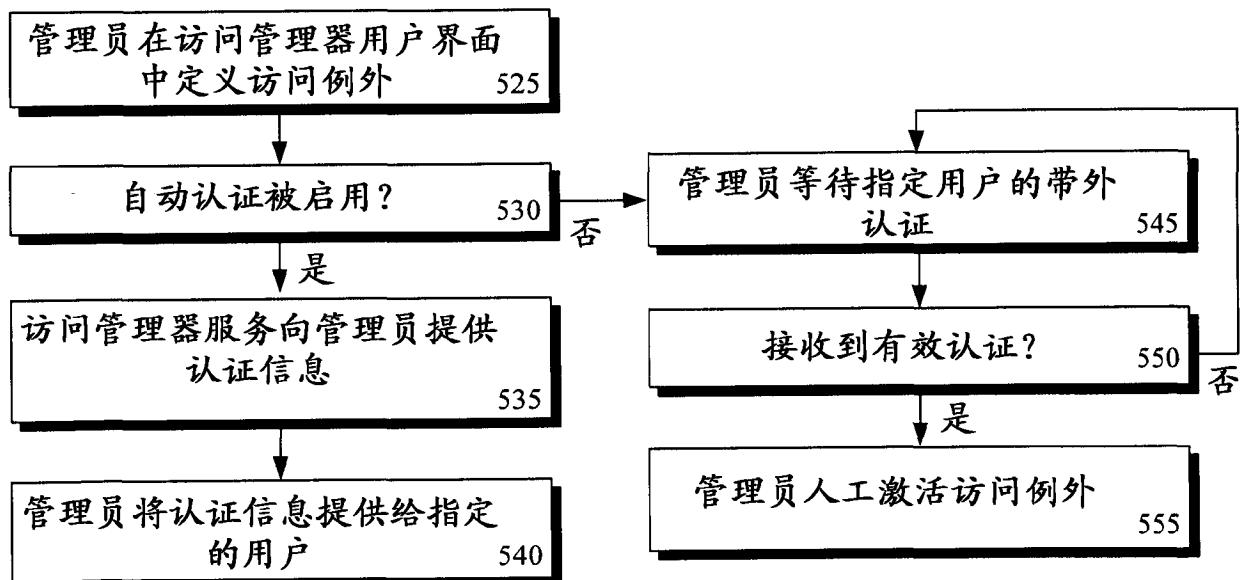
500520

图5