(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106407832 B
(45)授权公告日 2021.03.09

(21)申请号 201510481063.8

(22)申请日 2015.08.03

(65)同一申请的已公布的文献号
申请公布号 CN 106407832 A

(43)申请公布日 2017.02.15

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 原攀峰 张维 陈廷梁 何召卫

(74)专利代理机构 上海百一领御专利代理事务所(普通合伙) 31243
代理人 陈贞健

(51)Int.Cl.
G06F 21/62(2013.01)

(56)对比文件
CN 104378386 A,2015.02.25
CN 104378386 A,2015.02.25
CN 101377782 A,2009.03.04
US 2010250927 A1,2010.09.30

审查员 张琳

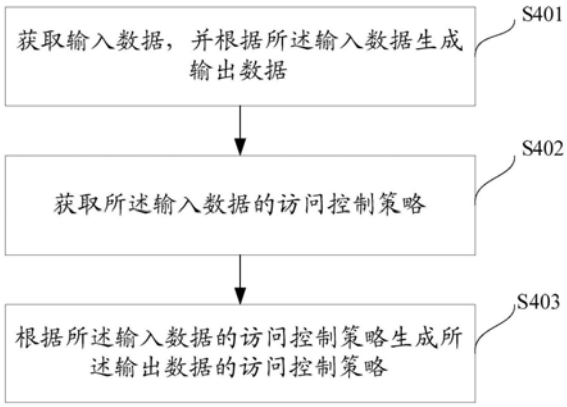
权利要求书2页 说明书14页 附图7页

(54)发明名称

一种用于数据访问控制的方法及设备

(57)摘要

本申请的目的是提供一种用于数据访问控制的方法及设备，具体地。获取输入数据，并根据所述输入数据生成输出数据；获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限。与现有技术相比，在将输出数据用于交换时，使得输出数据能够根据其上游的输入数据自动获得输出数据自身的访问控制策略，使得存在输入输出关系的输入数据和输出数据在传播性上具有一定的一致性，提高数据交换场景下数据访问控制的安全性。



CN 106407832 B

1.一种用于数据访问控制的方法,其中,该方法包括:

获取输入数据,并根据所述输入数据生成输出数据;

获取所述输入数据的访问控制策略,其中,所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限;

根据所述输入数据与输出数据之间的映射关系,并根据预设规则由所述输入数据的访问控制策略生成所述输出数据的访问控制策略,其中,所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限,所述预设规则包括以下任意一项:

对所述输入数据的访问控制策略中的访问权限求交集,作为所述输出数据的访问控制策略;或者

对所述输入数据的访问控制策略中的访问权限求并集,作为所述输出数据的访问控制策略。

2.根据权利要求1所述的方法,其中,获取输入数据,包括:

向数据提供方设备发送针对所述输入数据的授权请求,并在接收到所述数据提供方设备根据所述授权请求生成的针对所述输入数据的授权信息后,根据所述授权信息由存储设备获取所述输入数据。

3.根据权利要求2所述的方法,其中,获取所述输入数据的访问控制策略,包括:

向所述存储设备发送查询请求,并接收所述存储设备根据所述查询请求发送的所述输入数据的访问控制策略。

4.根据权利要求1所述的方法,其中,所述输入数据的访问控制策略包括用于控制设备对所述输入数据的多项访问权限,所述输出数据的访问控制策略包括用于控制设备对所述输出数据的多项访问权限;

所述预设规则包括以下任意一项:

分别对所述输入数据的访问控制策略中的多项访问权限求交集,作为所述输出数据的访问控制策略;或者

分别对所述输入数据的访问控制策略中的多项访问权限求并集,作为所述输出数据的访问控制策略。

5.根据权利要求1至4中任一项所述的方法,其中,根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略之后,还包括:

将所述输出数据及其对应的访问控制策略发送至存储设备。

6.根据权利要求5所述的方法,其中,将所述输出数据及其对应的访问控制策略发送至存储设备之后,还包括:

接收来自数据使用方设备的针对所述输入数据的授权请求,根据所述授权请求生成针对所述输入数据的授权信息,并向所述数据使用方设备发送所述授权信息,以使所述数据使用方设备根据所述授权信息由所述存储设备获取所述输出数据。

7.一种用于数据访问控制的设备,其中,该设备包括:

数据生成装置,用于获取输入数据,并根据所述输入数据生成输出数据;

策略获取装置,用于获取所述输入数据的访问控制策略,其中,所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限;

策略生成装置,用于根据所述输入数据与输出数据之间的映射关系,并根据预设规则

由所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限，所述预设规则包括以下任意一项：

对所述输入数据的访问控制策略中的访问权限求交集，作为所述输出数据的访问控制策略；或者

对所述输入数据的访问控制策略中的访问权限求并集，作为所述输出数据的访问控制策略。

8.根据权利要求7所述的设备，其中，所述数据生成装置，用于向数据提供方设备发送针对所述输入数据的授权请求，并在接收到所述数据提供方设备根据所述授权请求生成的针对所述输入数据的授权信息后，根据所述授权信息由存储设备获取输入数据，根据所述输入数据生成输出数据。

9.根据权利要求8所述的设备，其中，所述策略获取装置，用于向所述存储设备发送查询请求，并接收所述存储设备根据所述查询请求发送的所述输入数据的访问控制策略。

10.根据权利要求7所述的设备，其中，所述输入数据的访问控制策略包括用于控制设备对所述输入数据的多项访问权限，所述输出数据的访问控制策略包括用于控制设备对所述输出数据的多项访问权限；

所述策略生成装置中生成所述输出数据的访问控制策略的预设规则包括以下任意一项：

分别对所述输入数据的访问控制策略中的多项访问权限求交集，作为所述输出数据的访问控制策略；或者

分别对所述输入数据的访问控制策略中的多项访问权限求并集，作为所述输出数据的访问控制策略。

11.根据权利要求7至10中任一项所述的设备，其中，该设备还包括：

发送装置，用于在根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略之后，将所述输出数据及其对应的访问控制策略发送至存储设备。

12.根据权利要求11所述的设备，其中，该设备还包括：

授权处理装置，用于在将所述输出数据及其对应的访问控制策略发送至存储设备之后，接收来自数据使用方设备的针对所述输出数据的授权请求，根据所述授权请求生成针对所述输出数据的授权信息，并向所述数据使用方设备发送所述授权信息，以使所述数据使用方设备根据所述授权信息由所述存储设备获取所述输出数据。

一种用于数据访问控制的方法及设备

技术领域

[0001] 本申请涉及通信及计算机领域，尤其涉及一种用于数据访问控制的技术。

背景技术

[0002] 大数据时代背景下，数据的交换已成为必然的趋势。由于数据提供方对数据安全的需求以及特定数据的自身特点，在某些场景下，数据提供方希望能够对交换出去的数据进行安全的访问控制，如：数据是否允许被导出。另外，数据的交换与一般的商品交换不同，具有一些明显的特质，如数据的传播性等，这也对数据的安全控制带来了新的挑战。现有技术中进行安全访问控制的方式一般都是基于一个封闭环境(如企业的内部私有云)下，不涉及数据交换的场景，对于数据交换场景下的数据访问控制不能很好的支持，并且其采用的访问控制方式一般为使用一些特定的加密算法，对数据本身进行加密处理，对于大数据场景下数据普遍存在的传播性问题几乎没有考虑。

发明内容

[0003] 本申请的一个目的是提供一种用于数据访问控制的方法及设备，以解决现有技术中的数据访问控制方式不适用于数据交换场景的问题。

[0004] 为实现上述目的，本申请提供了一种用于数据访问控制的方法，该方法包括：

[0005] 获取输入数据，并根据所述输入数据生成输出数据；

[0006] 获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；

[0007] 根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限。

[0008] 进一步地，获取输入数据，包括：

[0009] 向数据提供方设备发送针对所述输入数据的授权请求，并在接收到所述数据提供方设备根据所述授权请求生成的针对所述输入数据的授权信息后，根据所述授权信息由存储设备获取所述输入数据。

[0010] 进一步地，获取所述输入数据的访问控制策略，包括：

[0011] 向所述存储设备发送查询请求，并接收所述存储设备根据所述查询请求发送的所述输入数据的访问控制策略。

[0012] 进一步地，根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，包括：

[0013] 根据所述输入数据与输出数据之间的映射关系，并根据预设规则由所述输入数据的访问控制策略生成所述输出数据的访问控制策略。

[0014] 进一步地，所述预设规则包括以下任意一项：

[0015] 对所述输入数据的访问控制策略中的访问权限求交集，作为所述输出数据的访问控制策略；或者

[0016] 对所述输入数据的访问控制策略中的访问权限求并集，作为所述输出数据的访问控制策略。

[0017] 进一步地，所述输入数据的访问控制策略包括用于控制设备对所述输入数据的多项访问权限，所述输出数据的访问控制策略包括用于控制设备对所述输出数据的多项访问权限；

[0018] 所述预设规则包括以下任意一项：

[0019] 分别对所述输入数据的访问控制策略中的多项访问权限求交集，作为所述输出数据的访问控制策略；或者

[0020] 分别对所述输入数据的访问控制策略中的多项访问权限求并集，作为所述输出数据的访问控制策略。

[0021] 进一步地，根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略之后，还包括：

[0022] 将所述输出数据及其对应的访问控制策略发送至存储设备。

[0023] 进一步地，将所述输出数据及其对应的访问控制策略发送至存储设备之后，还包括：

[0024] 接收来自数据使用方设备的针对所述输入数据的授权请求，根据所述授权请求生成针对所述输入数据的授权信息，并向所述数据使用方设备发送所述授权信息，以使所述数据使用方设备根据所述授权信息由所述存储设备获取所述输出数据。

[0025] 根据本申请的另一方面，还提供了一种用于数据访问控制的设备，该设备包括：

[0026] 数据生成装置，用于获取输入数据，并根据所述输入数据生成输出数据；

[0027] 策略获取装置，用于获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；

[0028] 策略生成装置，用于根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限。

[0029] 进一步地，所述数据生成装置，用于向数据提供方设备发送针对所述输入数据的授权请求，并在接收到所述数据提供方设备根据所述授权请求生成的针对所述输入数据的授权信息后，根据所述授权信息由存储设备获取输入数据，根据所述输入数据生成输出数据。

[0030] 进一步地，所述策略获取装置，用于向所述存储设备发送查询请求，并接收所述存储设备根据所述查询请求发送的所述输入数据的访问控制策略。

[0031] 进一步地，策略生成装置，用于根据所述输入数据与输出数据之间的映射关系，并根据预设规则由所述输入数据的访问控制策略生成所述输出数据的访问控制策略。

[0032] 进一步地，所述策略生成装置中生成所述输出数据的访问控制策略的预设规则包括以下任意一项：

[0033] 对所述输入数据的访问控制策略中的访问权限求交集，作为所述输出数据的访问控制策略；或者

[0034] 对所述输入数据的访问控制策略中的访问权限求并集，作为所述输出数据的访问控制策略。

[0035] 进一步地，所述输入数据的访问控制策略包括用于控制设备对所述输入数据的多

项访问权限，所述输出数据的访问控制策略包括用于控制设备对所述输出数据的多项访问权限；

[0036] 所述策略生成装置中生成所述输出数据的访问控制策略的预设规则包括以下任意一项：

[0037] 分别对所述输入数据的访问控制策略中的多项访问权限求交集，作为所述输出数据的访问控制策略；或者

[0038] 分别对所述输入数据的访问控制策略中的多项访问权限求并集，作为所述输出数据的访问控制策略。

[0039] 进一步地，该设备还包括：

[0040] 发送装置，用于在根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略之后，将所述输出数据及其对应的访问控制策略发送至存储设备。

[0041] 进一步地，该设备还包括：

[0042] 授权处理装置，用于在将所述输出数据及其对应的访问控制策略发送至存储设备之后，接收来自数据使用方设备的针对所述输出数据的授权请求，根据所述授权请求生成针对所述输出数据的授权信息，并向所述数据使用方设备发送所述授权信息，以使所述数据使用方设备根据所述授权信息由所述存储设备获取所述输出数据。

[0043] 本申请还提供了一种用于数据访问控制的设备，该设备包括：

[0044] 处理器；

[0045] 以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：获取输入数据，并根据所述输入数据生成输出数据；获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限。

[0046] 与现有技术相比，本申请提供的技术方案在获取输入数据后，根据所述输入数据生成输出数据，然后获取输入数据的访问控制策略，由于输出数据是根据输出数据生成，由此根据输入数据和输出数据之间的输入和输出关系，由输入数据的访问控制策略去生成输出数据的访问控制策略，在将输出数据用于交换时，使得输出数据能够根据其上游的输入数据自动获得输出数据自身的访问控制策略，使得存在输入输出关系的输入数据和输出数据在传播性上具有一定的一致性，提高数据交换场景下数据访问控制的安全性，适用于数据交换场景。

附图说明

[0047] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0048] 图1为本申请实施例提供的用于数据访问控制的设备的结构示意图；

[0049] 图2为本申请实施例提供的一种优选的用于数据访问控制的设备的结构示意图；

[0050] 图3为本申请实施例提供的一种更优选的用于数据访问控制的设备的结构示意图；

[0051] 图4为本申请实施例提供的用于数据访问控制的方法的流程图；

[0052] 图5为本申请实施例提供的一种优选的用于数据访问控制的方法的流程图；

[0053] 图6为本申请实施例提供的一种更优选的用于数据访问控制的方法的流程；

[0054] 图7为采用本申请实施例中数据访问控制方法的数据交易平台的结构示意图；

[0055] 图8为数据交易平台中数据提供方和数据使用方之间的交互流程图。

[0056] 附图中相同或相似的附图标记代表相同或相似的部件。

具体实施方式

[0057] 下面结合附图对本申请作进一步详细描述。

[0058] 在本申请一个典型的配置中，终端、服务网络的设备和可信方均包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0059] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0060] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0061] 图1示出了本申请实施例提供的一种用于数据访问控制的设备，其中，该设备1包括数据生成装置110、策略获取装置120以及策略生成装置130。具体地，数据生成装置110用于获取输入数据，并根据所述输入数据生成输出数据；策略获取装置120用于获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；策略生成装置130用于根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限。输入数据和输出数据之间具有输入和输出的映射关系，在将输出数据用于交换时，使得输出数据能够根据其上游的输入数据自动获得输出数据自身的访问控制策略，使得存在输入输出关系的输入数据和输出数据在传播性上具有一定的一致性，提高数据交换场景下数据访问控制的安全性，适用于数据交换场景。

[0062] 在此，设备1包括但不限于网络设备、用户设备或网络设备与用户设备通过网络相集成所构成的设备。在此，所述网络设备包括但不限于如网络主机、单个网络服务器、多个网络服务器集或基于云计算的计算机集合等实现；所述用户设备可以是运行于本地的用户端设备。在此，云由基于云计算(Cloud Computing)的大量主机或网络服务器构成，其中，云计算是分布式计算的一种，由一群松散耦合的计算机集组成的一个虚拟计算机。

[0063] 在某一数据交换的应用场景下，用户包括数据提供方以及数据使用方，对于某一用户，既可以数据提供方，同时也可以是数据使用方。其中，数据提供方向数据使用方提供数据，而数据使用方能够根据得到的数据生成新的数据，并且根据数据之间的输入和输出

关系获得新的数据的访问控制策略。此时所述设备1作为数据使用方设备，若数据提供方和数据使用方之间的数据交换通过云计算平台实现，则设备1可以是云计算平台中用于实现数据获取以及处理功能的一个服务器或者多个服务器的集合。在此，本领域技术人员应当能够理解，所述输入数据是指数据提供方提供的源数据，所述输出数据是指根据输入数据生成的数据。输入数据和输出数据包括但不限于：数据表、用户自定义函数、数据服务以及报表等，通过设定的访问控制策略，来控制设备对这些数据的访问权限。其中，访问权限可以根据具体的应用场景来设置，例如是否可以导出等。在此，所述输入数据可以是由多个数据提供方获取的多项不同的数据，也可以是数据使用方设备自身产生的数据，例如由数据提供方处购买的数据表，由数据提供方处购买的数据服务，或者数据使用方设备生成的用户自定义函数。

[0064] 当所述设备1作为数据使用方设备时，所述数据生成装置110用于向数据提供方设备发送针对所述输入数据的授权请求，并在接收到所述数据提供方设备根据所述授权请求生成的针对所述输入数据的授权信息后，根据所述授权信息由存储设备获取输入数据，根据所述输入数据生成输出数据。

[0065] 在此，针对输入数据的授权请求表示作为数据使用方的设备1希望获得输入数据使用权的请求，而对应的授权信息表示数据提供方设备同意数据使用方使用该数据的信息。若在实际应用场景中数据的交换采用交易的方式，则数据提供方将待出售的数据在云计算平台提供的数据市场中上架，使得数据使用方能够获知当前有哪些数据当前可以购买。所述存储设备可以是云计算平台中用于实现数据存储处理功能的一个服务器或者多个服务器的集合，数据提供方在数据市场中上架的数据被存储在所述存储设备中。在进行数据交换时，数据使用方和数据提供方之间并不直接进行数据的交换，数据使用方如需要获得某一上架的数据，会向数据提供方发送一个购买该数据的购买申请(即为授权请求)，数据提供方在收到购买申请后，若同意该次购买，则会向数据使用方发送一个同意购买的审批信息(即为授权信息)，此时数据使用方就可以根据同意购买的审批信息区向云计算平台中用于存储数据的存储设备请求获取对应的数据，由此完成数据的获取。由于数据提供方和数据使用方之间通过申请和授权的方式交换数据，适用于云计算平台下大数据处理的应用场景，即使不对数据本身进行加密，数据传播的安全性也能够得到有效控制。

[0066] 根据所述输入数据生成输出数据时，根据数据的实际处理目的，可以采用不同的生成方式，包括但不限于：对数据进行统计分析(例如ETL，Extract Transform Load，数据抽取、转换、加载)，或者对数据进行数据挖掘等。例如，所述输入数据为由数据提供方A处购买的数据表，对该数据表进行统计分析，抽取数据表中的某几项数据，然后对数据进行转换(例如对数据格式进行转换)后，再将转换后的数据加载至新的数据表，从而生成一张新的数据表(即为输出数据)。再如，所述输入数据包括分别由数据提供方A、B、C处购买的数据表A、数据表B以及数据服务C，其中，数据表A为多个城市未来几天的气温数据，数据表B为这几个城市未来几天内的降雨概率数据，数据服务C为根据气温以及降雨概率对雨伞销量的趋势预测，通过上述数据，可以生成数据表D，该数据表D包含的数据为几个城市中未来几天内雨伞的销量的预测数据。在此，本领域技术人员应能理解上述关于输出数据的生成方式仅为举例，其他现有的或今后可能出现的方式如可适用于本申请，也应包含在本申请保护范围以内，并在此以引用方式包含于此。

[0067] 在上述应用场景下，输入数据的访问控制策略可以独立于输入数据进行存储，此时在数据生成装置完成输出数据的生成后，所述策略获取装置120向所述存储设备发送查询请求，并接收所述存储设备根据所述查询请求发送的所述输入数据的访问控制策略。仍以前述数据表A、数据表B以及数据服务C生成数据表D的场景为例，在数据表A、数据表B以及数据服务C上架时，数据提供方已将这些数据的访问控制策略提交至云计算平台中用于存储数据的服务器(即存储设备)中，在生成数据表D后，设备1的策略获取装置会向存储设备进行查询，以获取输入数据的访问控制策略。

[0068] 具体地，策略生成装置130根据所述输入数据与输出数据之间的映射关系，并根据预设规则由所述输入数据的访问控制策略生成所述输出数据的访问控制策略。由于输出数据的访问控制策略是基于输入数据和输出数据的映射关系生成，使得对于输入数据和输出数据其访问权限存在一定的延续性。接上例，数据表D对应的输入数据为数据表A、数据表B以及数据服务C，其预设规则可以根据数据的特点以及业务需求来设置，例如数据表A内包含了较为敏感的数据，不适合让用户随意导出使用，其设置的访问控制策略为不允许导出，那么可以采用严格控制的预设规则：即对输入数据的访问控制策略中的访问权限求交集，作为输出数据的访问控制策略。此时，即使数据表B和数据服务C的访问控制策略为允许导出，数据表D仍然为不可导出。当然，也可以采用宽松控制的预设规则：即对输入数据的访问控制策略中的访问权限求并集，作为输出数据的访问控制策略。此时，数据表A、数据表B以及数据服务C中只要有一个采用了允许导出，那么生成的数据表D也允许导出。在此，本领域技术人员应能理解上述预设规则仅为举例，其他现有的或今后可能出现的其它形式的预设规则如可适用于本申请，也应包含在本申请保护范围以内，并在此以引用方式包含于此。

[0069] 根据应用场景的不同，所述输入数据的访问控制策略包括用于控制设备对所述输入数据的多项访问权限，所述输出数据的访问控制策略包括用于控制设备对所述输出数据的多项访问权限，以适应不同应用场景的需求。以本申请实施例中提及的数据交易的场景为例，访问控制策略包含的访问权限可以包括但不限于：是否允许上架，是否允许导出，是否允许在开发环境访问等。其中，允许上架是指数据提供方可以将该数据在数据市场中上架，即可以将该数据及由此生成的数据授权给数据使用方。所述开发环境是指数据提供方内部进行数据开发或者分析的私有环境。一般在数据交易的场景下，数据由各个数据提供方进行生产，数据生产的过程即为由输入数据生成输出数据的过程。在生成过程中，可以从其它数据提供方购买的数据中提取样本数据，来进行相关的数据开发或者分析，以生成输出数据。允许在开发环境访问是指在对数据进行开发或者分析时，没有任何限制，可以提取将该数据的全部内容作为样本数据，若不允许在开发环境访问，则开发或者分析时不能直接获取到数据的内容，只能获取到预先根据该数据的内容提取的样本数据，来进行开发或者分析。

[0070] 当输入数据的访问控制策略包含多项访问权限时，对应的严格控制的预设规则和宽松控制的预设规则分为别：分别对所述输入数据的访问控制策略中的多项访问权限求交集，作为所述输出数据的访问控制策略；以及分别对所述输入数据的访问控制策略中的多项访问权限求并集，作为所述输出数据的访问控制策略。以数据表E、数据表F、数据表G、数据表H、数据表I为例，其输入输出的映射关系为：(E、F、G)→(H、I)，即由数据表E～G，生成了两张新的数据表H、I。假设其访问控制策略定义如下：AP1，是否允许上架；AP2，是否允许导

出;AP3,是否允许在开发环境访问,那么

[0071] 数据表E(AP1,AP2,AP3)＝(1,0,0);

[0072] 数据表F(AP1,AP2,AP3)＝(1,1,0);

[0073] 数据表G(AP1,AP2,AP3)＝(1,1,1);

[0074] 那么根据严格控制的预设规则,生成的数据表H和数据表I的访问控制策略为:数据表H、I(AP1,AP2,AP3)＝(1,0,0)∩(1,1,0)∩(1,1,1)＝(1,0,0),即仅允许上架,而不允许导出以及在开发环境访问。对应地,根据宽松控制的预设规则,生成的数据表H和数据表I的访问控制策略为:数据表H、I(AP1,AP2,AP3)＝(1,0,0)∪(1,1,0)∪(1,1,1)＝(1,1,1),即允许上架、允许导出并且允许在开发环境访问。通过设置不同的预设规则以及多项不同的访问权限,使得数据访问控制的粒度较细,从而满足大数据云计算平台下灵活多样的访问控制需求。

[0075] 进一步地,本申请实施例还提供了一种优选的用于数据访问控制的设备1,由于在生成输出数据以及输出数据的访问控制策略后,设备1也可以作为数据提供方,将其生产的输出数据进行上架,授权给其它数据使用方使用,使得技术方案更适用于云计算平台的数据交换的应用场景。所述设备1的结构如图2所示,除图1示出的数据生成装置110、策略获取装置120、策略生成装置130之外,还包括发送装置140。具体地,所述发送装置140在根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略之后,将所述输出数据及其对应的访问控制策略发送至存储设备。在此,本领域技术人员应当理解,数据生成装置110、策略获取装置120和策略生成装置130分别与图1实施例中对应装置的内容相同或基本相同,为简明起见,故在此不再赘述,并以引用的方式包含于此。

[0076] 在上述应用场景中,若设备1生成的数据表H和数据表I均允许上架,则设备1可以将所述数据表H、数据表I及其对应的访问控制策略发送至存储设备,使得其它数据使用方提出使用数据表H和数据表I的购买申请,以完成数据的交易。

[0077] 进一步地,本申请实施例还提供了一种更优选的用于数据访问控制的设备1,该设备1的结构如图3所示,除图2示出的数据生成装置110、策略获取装置120、策略生成装置130和发送装置140之外,还包括授权处理装置150,以完成对于其它数据使用方提出的授权请求的审批。具体地,授权处理装置150在将所述输出数据及其对应的访问控制策略发送至存储设备之后,接收来自数据使用方设备的针对所述输出数据的授权请求,根据所述授权请求生成针对所述输出数据的授权信息,并向所述数据使用方设备发送所述授权信息,以使所述数据使用方设备根据所述授权信息由所述存储设备获取所述输出数据。在此,本领域技术人员应当理解,数据生成装置110、策略获取装置120、策略生成装置130、发送装置140分别与图2实施例中对应装置的内容相同或基本相同,为简明起见,故在此不再赘述,并以引用的方式包含于此。

[0078] 其中,所述针对输出数据的授权请求、授权信息与前述的针对输入数据的授权请求、授权信息的表示的内容基本相同,其区别仅在于此时设备1所表示的是数据提供方设备,该输出数据被其它数据使用方获取后,作为其它数据使用方的进行数据生成的输入数据被使用。在上述应用场景中,若数据使用方需要购买数据表H,那么数据提供方就会接收到来自针对数据表H的购买请求,若同意该次购买,则会向数据使用方发送一个同意购买的审批信息。数据提供方和数据使用方之间通过申请和授权的方式交换数据,适用于云计算

平台下大数据处理的应用场景，即使不对数据本身进行加密，数据传播的安全性也能够得到有效控制。

[0079] 在此，本领域技术人员应当能够理解，在云计算平台中，任意用户的数据处理操作均可以由云计算平台内的计算机集群完成，例如利用虚拟机技术，数据提供方设备、数据使用方设备所执行的数据处理操作均可以由计算机集群内的实现类似功能的实体设备集合完成(例如具有数据处理以及收发功能的服务器)，而用户的本地设备可以仅仅实现接入所述云计算平台的应用接口的功能。

[0080] 图4示出了本申请实施例提供的一种用于数据访问控制的方法，该方法包括以下步骤：

[0081] 步骤S401，获取输入数据，并根据所述输入数据生成输出数据；

[0082] 步骤S402，获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；

[0083] 步骤S403，根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限。

[0084] 由于输入数据和输出数据之间具有输入和输出的映射关系，在将输出数据用于交换时，使得输出数据能够根据其上游的输入数据自动获得输出数据自身的访问控制策略，使得存在输入输出关系的输入数据和输出数据在传播性上具有一定的一致性，提高数据交换场景下数据访问控制的安全性。

[0085] 在某一数据交换的应用场景下，用户包括数据提供方以及数据使用方，对于某一用户，既可以数据提供方，同时也可以是数据使用方。其中，数据提供方向数据使用方提供数据，而数据使用方能够根据得到的数据生成新的数据，并且根据数据之间的输入和输出关系获得新的数据的访问控制策略。在此，前述用于数据访问控制的方法的执行主体是作为数据使用方设备，若数据提供方和数据使用方之间的数据交换通过云计算平台实现，则执行上述方法的数据使用方设备可以是云计算平台中用于实现数据获取以及处理功能的一个服务器或者多个服务器的集合。在此，本领域技术人员应当能够理解，所述输入数据是指数据提供方提供的源数据，所述输出数据是指根据输入数据生成的数据。输入数据和输出数据包括但不限于：数据表、用户自定义函数、数据服务以及报表等，通过设定的访问控制策略，来控制包括设备对这些数据的访问权限。其中，访问权限可以根据具体的应用场景来设置，例如是否可以导出等。在此，所述输入数据可以是由多个数据提供方获取的多项不同的数据，也可以是数据使用方设备自身产生的数据，例如由数据提供方处购买的数据表，由数据提供方处购买的数据服务，或者数据使用方设备生成的用户自定义函数。

[0086] 当作为数据使用方时，步骤S101中获取输入数据，具体包括于向数据提供方设备发送针对所述输入数据的授权请求，并在接收到所述数据提供方设备根据所述授权请求生成的针对所述输入数据的授权信息后，根据所述授权信息由存储设备获取输入数据。

[0087] 在此，针对输入数据的授权请求表示作为数据使用方希望获得输入数据使用权的请求，而对应的授权信息表示数据提供方同意数据使用方使用该数据的信息。若在实际应用场景中数据的交换采用交易的方式，则数据提供方将待出售的数据在云计算平台提供的数据市场中上架，使得数据使用方能够获知当前有哪些数据当前可以购买。所述存储设备可以是云计算平台中用于实现数据存储处理功能的一个服务器或者多个服务器的集合，数

据提供方在数据市场中上架的数据被存储在所述存储设备中。在进行数据交换时，数据使用方和数据提供方之间并不直接进行数据的交换，数据使用方如需要获得某一上架的数据，会向数据提供方发送一个购买该数据的购买申请(即为授权请求)，数据提供方在收到购买申请后，若同意该次购买，则会向数据使用方发送一个同意购买的审批信息(即为授权信息)，此时数据使用方就可以根据同意购买的审批信息区向云计算平台中用于存储数据的存储设备请求获取对应的数据，由此完成数据的获取。由于数据提供方和数据使用方之间通过申请和授权的方式交换数据，适用于云计算平台下大数据处理的应用场景，即使不对数据本身进行加密，数据传播的安全性也能够得到有效控制。

[0088] 根据所述输入数据生成输出数据时，根据数据的实际处理目的，可以采用不同的生成方式，包括但不限于：对数据进行统计分析(例如ETL，Extract Transform Load，数据抽取、转换、加载)，或者对数据进行数据挖掘等。例如，所述输入数据为由数据提供方A处购买的数据表，对该数据表进行统计分析，抽取数据表中的某几项数据，然后对数据进行转换(例如对数据格式进行转换)后，再将转换后的数据加载至新的数据表，从而生成一张新的数据表(即为输出数据)。再如，所述输入数据包括分别由数据提供方A、B、C处购买的数据表A、数据表B以及数据服务C，其中，数据表A为多个城市未来几天的气温数据，数据表B为这几个城市未来几天内的降雨概率数据，数据服务C为根据气温以及降雨概率对雨伞销量的趋势预测，通过上述数据，可以生成数据表D，该数据表D包含的数据为几个城市中未来几天内雨伞的销量的预测数据。在此，本领域技术人员应能理解上述关于输出数据的生成方式仅为举例，其他现有的或今后可能出现的方式如可适用于本申请，也应包含在本申请保护范围以内，并在此以引用方式包含于此。

[0089] 在上述应用场景下，输入数据的访问控制策略可以独立于输入数据进行存储，此时在完成输出数据的生成后，步骤S102获取所述输入数据的访问控制策略，具体包括：向所述存储设备发送查询请求，并接收所述存储设备根据所述查询请求发送的所述输入数据的访问控制策略。仍以前述数据表A、数据表B以及数据服务C生成数据表D的场景为例，在数据表A、数据表B以及数据服务C上架时，数据提供方已将这些数据的访问控制策略提交至云计算平台中用于存储数据的服务器(即存储设备)中，在生成数据表D后，会向存储设备进行查询，以获取输入数据的访问控制策略。

[0090] 具体地，步骤S103根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，包括：根据所述输入数据与输出数据之间的映射关系，并根据预设规则由所述输入数据的访问控制策略生成所述输出数据的访问控制策略。由于输出数据的访问控制策略是基于输入数据和输出数据的映射关系生成，使得对于输入数据和输出数据其访问权限存在一定的延续性。接上例，数据表D对应的输入数据为数据表A、数据表B以及数据服务C，其预设规则可以根据数据的特点以及业务需求来设置，例如数据表A内包含了较为敏感的数据，不适合让用户随意导出使用，其设置的访问控制策略为不允许导出，那么可以采用严格控制的预设规则：即对输入数据的访问控制策略中的访问权限求交集，作为输出数据的访问控制策略。此时，即使数据表B和数据服务C的访问控制策略为允许导出，数据表D仍然为不可导出。当然，也可以采用宽松控制的预设规则：即对输入数据的访问控制策略中的访问权限求并集，作为输出数据的访问控制策略。此时，数据表A、数据表B以及数据服务C中只要有一个采用了允许导出，那么生成的数据表D也允许导出。在此，本领域技术人员应能理解上

述预设规则仅为举例，其他现有的或今后可能出现的其它形式的预设规则如可适用于本申请，也应包含在本申请保护范围以内，并在此以引用方式包含于此。

[0091] 根据应用场景的不同，所述输入数据的访问控制策略包括用于控制设备对所述输入数据的多项访问权限，所述输出数据的访问控制策略包括用于控制设备对所述输出数据的多项访问权限，以适应不同应用场景的需求。以本申请实施例中提及的数据交易的场景为例，访问控制策略包含的访问权限可以包括但不限于：是否允许上架，是否允许导出，是否允许在开发环境访问等。其中，允许上架是指数据提供方可以将该数据在数据市场中上架，即可以将该数据及由此生成的数据授权给数据使用方。所述开发环境是指数据提供方内部进行数据开发或者分析的私有环境。一般在数据交易的场景下，数据由各个数据提供方进行生产，数据生产的过程即为由输入数据生成输出数据的过程。在生成过程中，可以从其它数据提供方购买的数据中提取样本数据，来进行相关的数据开发或者分析，以生成输出数据。允许在开发环境访问是指在对数据进行开发或者分析时，没有任何限制，可以提取将该数据的全部内容作为样本数据，若不允许在开发环境访问，则开发或者分析时不能直接获取到数据的内容，只能获取到预先根据该数据的内容提取的样本数据，来进行开发或者分析。

[0092] 当输入数据的访问控制策略包含多项访问权限时，对应的严格控制的预设规则和宽松控制的预设规则分为别：分别对所述输入数据的访问控制策略中的多项访问权限求交集，作为所述输出数据的访问控制策略；以及分别对所述输入数据的访问控制策略中的多项访问权限求并集，作为所述输出数据的访问控制策略。以数据表E、数据表F、数据表G、数据表H、数据表I为例，其输入输出的映射关系为：(E、F、G)→(H、I)，即由数据表E～G，生成了两张新的数据表H、I。假设其访问控制策略定义如下：AP1，是否允许上架；AP2，是否允许导出；AP3，是否允许在开发环境访问，那么

[0093] 数据表E(AP1,AP2,AP3)＝(1,0,0)；

[0094] 数据表F(AP1,AP2,AP3)＝(1,1,0)；

[0095] 数据表G(AP1,AP2,AP3)＝(1,1,1)；

[0096] 那么根据严格控制的预设规则，生成的数据表H和数据表I的访问控制策略为：数据表H、I(AP1,AP2,AP3)＝(1,0,0)∩(1,1,0)∩(1,1,1)＝(1,0,0)，即仅允许上架，而不允许导出以及在开发环境访问。对应地，根据宽松控制的预设规则，生成的数据表H和数据表I的访问控制策略为：数据表H、I(AP1,AP2,AP3)＝(1,0,0)∪(1,1,0)∪(1,1,1)＝(1,1,1)，即允许上架、允许导出并且允许在开发环境访问。通过设置不同的预设规则以及多项不同的访问权限，使得数据访问控制的粒度较细，从而满足大数据云计算平台下灵活多样的访问控制需求。

[0097] 进一步地，本申请实施例还提供了一种优选的用于数据访问控制的方法，若某一用户使用该方法生成输出数据以及输出数据的访问控制策略后，该也可以作为数据提供方，将其生产的输出数据作上架，授权给其它数据使用方使用，使得技术方案更适用于云计算平台的数据交换的应用场景。由此，该方法处理流程如图5所示，包括以下步骤：

[0098] 步骤S501，获取输入数据，并根据所述输入数据生成输出数据；

[0099] 步骤S502，获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；

[0100] 步骤S503，根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限；

[0101] 步骤S504，将所述输出数据及其对应的访问控制策略发送至存储设备。

[0102] 例如，在上述应用场景中，若生成的数据表H和数据表I均允许上架，则用户可以将所述数据表H、数据表I及其对应的访问控制策略发送至存储设备，使得其它数据使用方提出使用数据表H和数据表I的购买申请，以完成数据的交易。

[0103] 进一步地，本申请实施例还提供了一种更优选的用于数据访问控制的方法，该方法的处理流程如图6所示，包括以下步骤：

[0104] 步骤S601，获取输入数据，并根据所述输入数据生成输出数据；

[0105] 步骤S602，获取所述输入数据的访问控制策略，其中，所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限；

[0106] 步骤S603，根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略，其中，所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限；

[0107] 步骤S604，将所述输出数据及其对应的访问控制策略发送至存储设备；

[0108] 步骤S605，接收来自数据使用方设备的针对所述输出数据的授权请求，根据所述授权请求生成针对所述输出数据的授权信息，并向所述数据使用方设备发送所述授权信息，以使所述数据使用方设备根据所述授权信息由所述存储设备获取所述输出数据。

[0109] 其中，所述针对输出数据的授权请求、授权信息与前述的针对输入数据的授权请求、授权信息的表示的内容基本相同，其区别仅在于该方法的执行主体在执行步骤S605时是作为数据提供方设备，该输出数据被其它数据使用方获取后，作为其它数据使用方的进行数据生成的输入数据被使用。在上述应用场景中，若数据使用方需要购买数据表H，那么数据提供方就会接收到来自针对数据表H的购买请求，若同意该次购买，则会向数据使用方发送一个同意购买的审批信息。数据提供方和数据使用方之间通过申请和授权的方式交换数据，适用于云计算平台下大数据处理的应用场景，即使不对数据本身进行加密，数据传播的安全性也能够得到有效控制。

[0110] 在此，本领域技术人员应当能够理解，在云计算平台中，任意用户的数据处理操作均可以由云计算平台内的计算机集群完成，例如利用虚拟机技术，数据提供方设备和数据使用方设备所执行的数据处理操作均可以由计算机集群内的实现类似功能的实体设备集合完成(例如具有数据处理以及收发功能的服务器)，而用户的本地设备可以仅仅实现接入所述云计算平台的应用接口的功能。

[0111] 图7示出了采用上述数据访问控制方法的云计算环境下的数据交易平台，该平台的功能框架如图7所示，包括了以下几个功能模块：数据库模块710、数据交换发布模块720、数据加工任务模块730、实时血缘采集模块740、安全访问控制模块750、访问控制策略查询模块760、数据库模块710、数据交换发布模块720、数据加工任务模块730、实时血缘采集模块740、安全访问控制模块750以及访问控制策略查询模块760。上述功能模块中，数据库模块710用于实现前述存储设备的相关功能，而其余功能模块则用于实现设备1在作为数据使用方设备或者数据提供方设备时的相应功能，其具体实现可以是于云计算平台中实现特定功能的计算机或者计算机集群。对于某一用户，在作为数据提供方或者数据使用方使用该数据交易平台实现数据交易以及进行数据访问控制时，可以使用用户本地设备(例如本地

计算机、移动终端等)提供的应用接口接入云计算平台中实现特定功能的计算机或者计算机集群,以实现上述功能模块的相关功能。

[0112] 具体地,数据库模块710用于保存交易数据、交易数据对应的访问控制策略、以及其它功能模块在运行过程中产生的运行数据等,在云计算环境下,数据库模块可以采用分布式的数据库。其中,所述交易数据为数据提供方和数据使用方之间交换的数据,对于某一用户其购买到的交易数据即为前述的输入数据,该用户生成的、且上架进行交换的交易数据即为前述的输出数据。

[0113] 数据交换发布模块720用于发布数据以进行数据交换,设置交易数据的访问控制策略,使得交易数据上架,可以被其它用户申请购买,并且根据授权信息向数据使用方发放交易数据。

[0114] 数据加工任务模块730用于对交换得到的数据进行加工处理,即前述方法中根据输入数据生成输出数据,由于一般情况下生成的方式可以通过程序预先设定,因此数据加工处理任务可以由工作流调度周期性的执行。

[0115] 实时血缘采集模块740用于在完成数据加工处理后,采集血缘关系,其中血缘关系表示输入数据和输出数据之间的映射关系,即指示了由哪些数据生成了哪些数据。

[0116] 安全访问控制模块750用于通过解析血缘关系,得到输入数据和输出数据之间的映射关系,然后查询输入数据的访问控制策略,并根据输入数据和输出数据之间的映射关系以及输入数据的访问控制策略,计算输出数据的访问控制策略。其中,计算输出数据的访问控制策略的规则已经在前述部分提及,此处不再赘述。

[0117] 访问控制策略查询模块760对外提供应用程序接口,使得用户在使用这些交易数据时,能够通过应用程序接口查询数据的访问控制策略,并根据访问控制策略进行数据的安全访问控制,以保证数据在传播过程中的安全性。

[0118] 此外,本申请实施例还提供了一种用于数据访问控制的设备,该设备包括:

[0119] 处理器;

[0120] 以及被安排成存储计算机可执行指令的存储器,所述可执行指令在被执行时使所述处理器:获取输入数据,并根据所述输入数据生成输出数据;获取所述输入数据的访问控制策略,其中,所述输入数据的访问控制策略用于控制设备对所述输入数据的访问权限;根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略,其中,所述输出数据的访问控制策略用于控制设备对所述输出数据的访问权限。

[0121] 图8示出了用户使用前述云计算环境下的数据交易平台的交互流程图,进行交互的两个用户分别作为数据提供方和数据使用方。

[0122] 对于数据提供方,其处理流程包括:

[0123] 步骤S801,选择要上架的数据,例如选择一张要发布到数据市场的数据表。

[0124] 步骤S802,确定该数据的访问控制策略,然后通过数据交换发布模块720提交并存储到云计算平台的数据库模块710中。

[0125] 步骤S803,进行数据交换。

[0126] 对于数据提供方,进行数据交换的步骤具体为:等待数据使用方的购买申请,在接收到购买申请后,可以进行审批,以同意数据使用方获得该数据。

[0127] 对于数据使用方,其处理流程包括:

[0128] 步骤S803,进行数据交换。

[0129] 对于数据使用方,进行数据交换的步骤具体为:在数据市场上架的数据中发现需要购买的数据后,向数据提供方发送购买申请,在收到数据提供方同意购买的审批后,由云计算平台的数据库模块710获取该数据。

[0130] 步骤S804,使用交换得到数据,将其作为输入数据,并通过数据加工任务模块730进行数据加工处理,以生成新的输出数据。

[0131] 步骤S805,通过血缘采集模块740采集数据的血缘关系。

[0132] 步骤S806,通过安全访问控制模块750解析血缘关系,得到输入数据和输出数据之间的映射关系。

[0133] 步骤S807,通过访问控制策略查询模块760从云计算平台查询输入数据的访问控制策略。

[0134] 步骤S808,通过安全访问控制模块750,根据预设规则计算得到输出数据的访问控制策略,例如按照严格控制的预设规则,对所述输入数据的访问控制策略中的访问权限求并集,作为所述输出数据的访问控制策略。

[0135] 步骤S809,将输出数据的访问控制策略存储到云计算平台的数据库模块710中,供需要使用该数据的用户通过应用程序接口查询使用。

[0136] 综上所述,本申请提供的技术方案在获取输入数据后,根据所述输入数据生成输出数据,然后获取输入数据的访问控制策略,由于输出数据是根据输出数据生成,由此根据输入数据和输出数据之间的输入和输出关系,由输入数据的访问控制策略去生成输出数据的访问控制策略,在将输出数据用于交换时,使得输出数据能够根据其上游的输入数据自动获得输出数据自身的访问控制策略,使得存在输入输出关系的输入数据和输出数据在传播性上具有一定的一致性,提高数据交换场景下数据访问控制的安全性。此外,通过设置不同的预设规则以及多项不同的访问权限,使得数据访问控制的粒度较细,从而满足大数据云计算平台下灵活多样的访问控制需求。

[0137] 需要注意的是,本申请可在软件和/或软件与硬件的组合体中被实施,例如,可采用专用集成电路(ASIC)、通用目的计算机或任何其他类似硬件设备来实现。在一个实施例中,本申请的软件程序可以通过处理器执行以实现上文所述步骤或功能。同样地,本申请的软件程序(包括相关的数据结构)可以被存储到计算机可读记录介质中,例如,RAM存储器,磁或光驱动器或软磁盘及类似设备。另外,本申请的一些步骤或功能可采用硬件来实现,例如,作为与处理器配合从而执行各个步骤或功能的电路。

[0138] 另外,本申请的一部分可被应用为计算机程序产品,例如计算机程序指令,当其被计算机执行时,通过该计算机的操作,可以调用或提供根据本申请的方法和/或技术方案。而调用本申请的方法的程序指令,可能被存储在固定的或可移动的记录介质中,和/或通过广播或其他信号承载媒体中的数据流而被传输,和/或被存储在根据所述程序指令运行的计算机设备的工作存储器中。在此,根据本申请的一个实施例包括一个装置,该装置包括用于存储计算机程序指令的存储器和用于执行程序指令的处理器,其中,当该计算机程序指令被该处理器执行时,触发该装置运行基于前述根据本申请的多个实施例的方法和/或技术方案。

[0139] 对于本领域技术人员而言,显然本申请不限于上述示范性实施例的细节,而且在

不背离本申请的精神或基本特征的情况下，能够以其他的具体形式实现本申请。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本申请的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本申请内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外，显然“包括”一词不排除其他单元或步骤，单数不排除复数。装置权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。

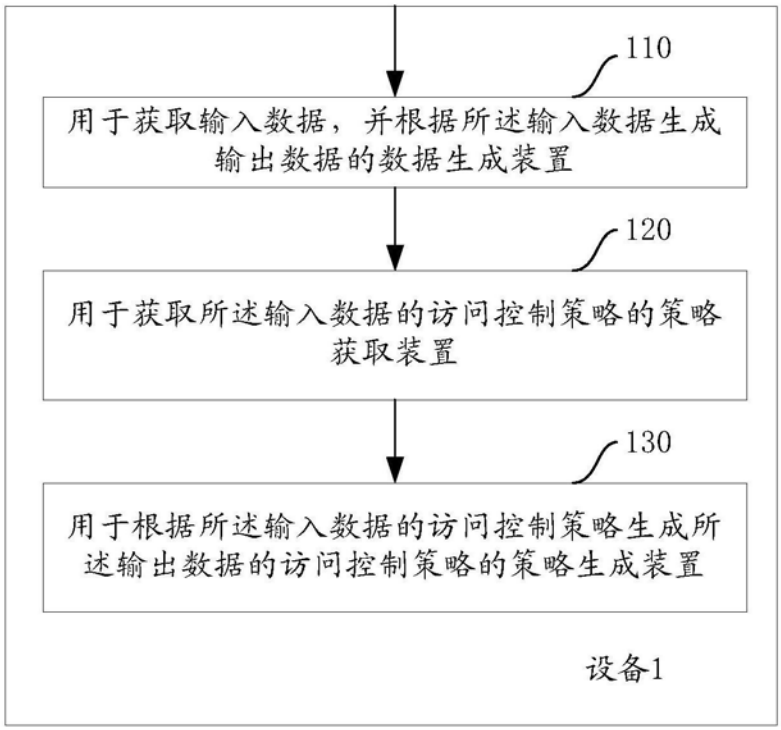

110
用于获取输入数据，并根据所述输入数据生成输出数据的数据生成装置
120
用于获取所述输入数据的访问控制策略的策略获取装置
130
用于根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略的策略生成装置
设备1

图1

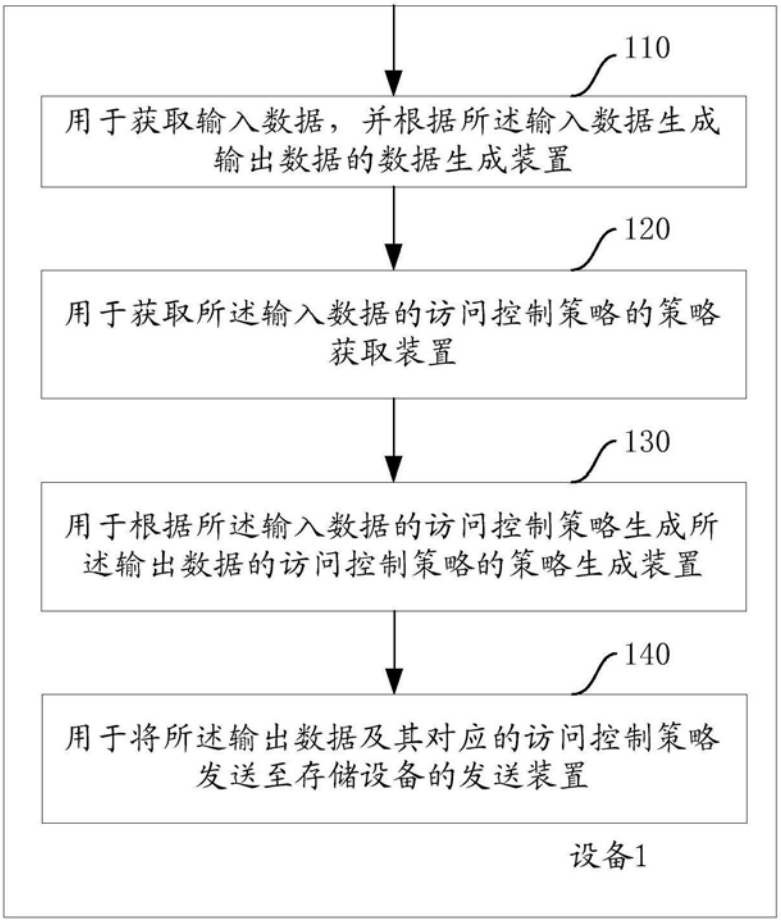

110
用于获取输入数据，并根据所述输入数据生成输出数据的数据生成装置
120
用于获取所述输入数据的访问控制策略的策略获取装置
130
用于根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略的策略生成装置
140
用于将所述输出数据及其对应的访问控制策略发送至存储设备的发送装置
设备1

图2

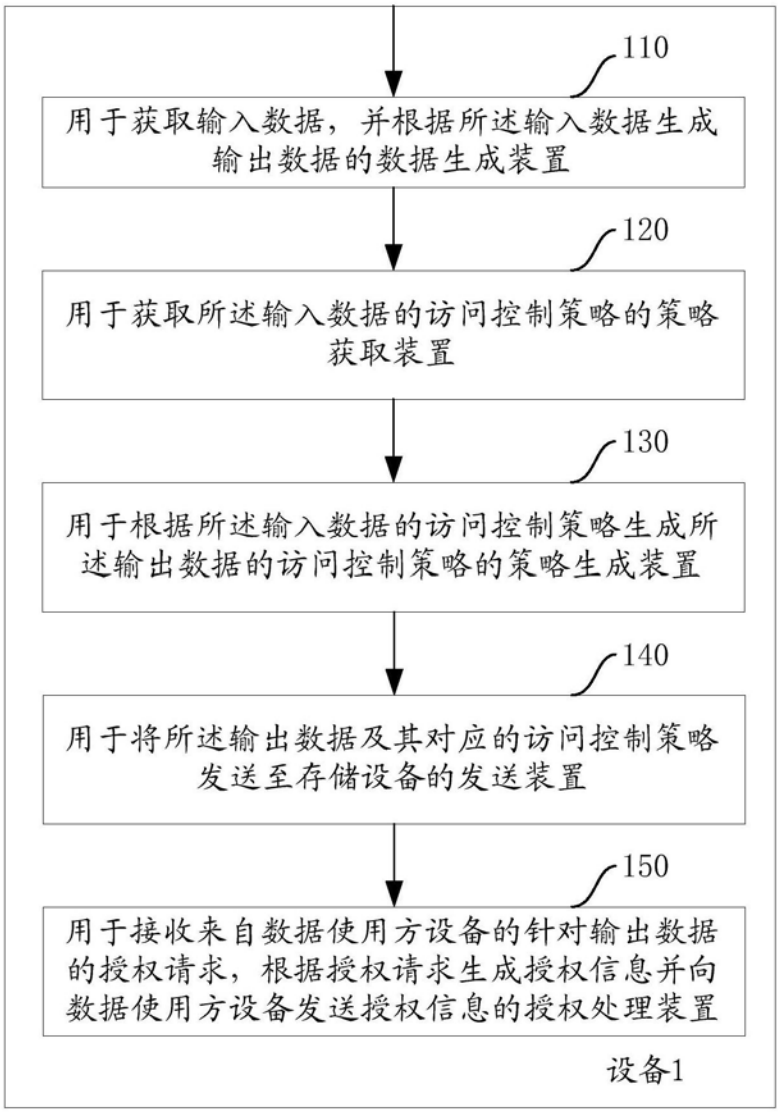

110
用于获取输入数据，并根据所述输入数据生成输出数据的数据生成装置
120
用于获取所述输入数据的访问控制策略的策略获取装置
130
用于根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略的策略生成装置
140
用于将所述输出数据及其对应的访问控制策略发送至存储设备的发送装置
150
用于接收来自数据使用方设备的针对输出数据的授权请求，根据授权请求生成授权信息并向数据使用方设备发送授权信息的授权处理装置
设备1

图3

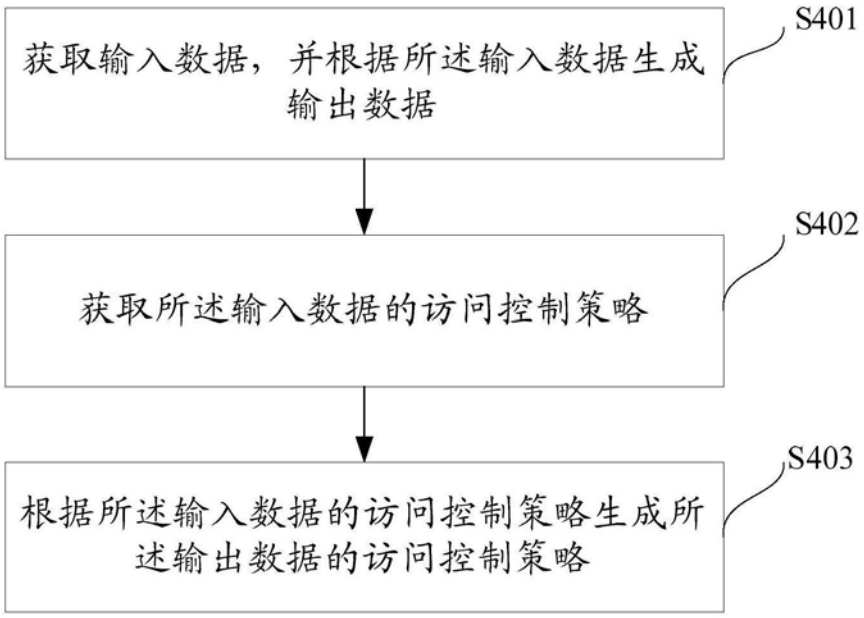

S401
获取输入数据，并根据所述输入数据生成输出数据
S402
获取所述输入数据的访问控制策略
S403
根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略

图4

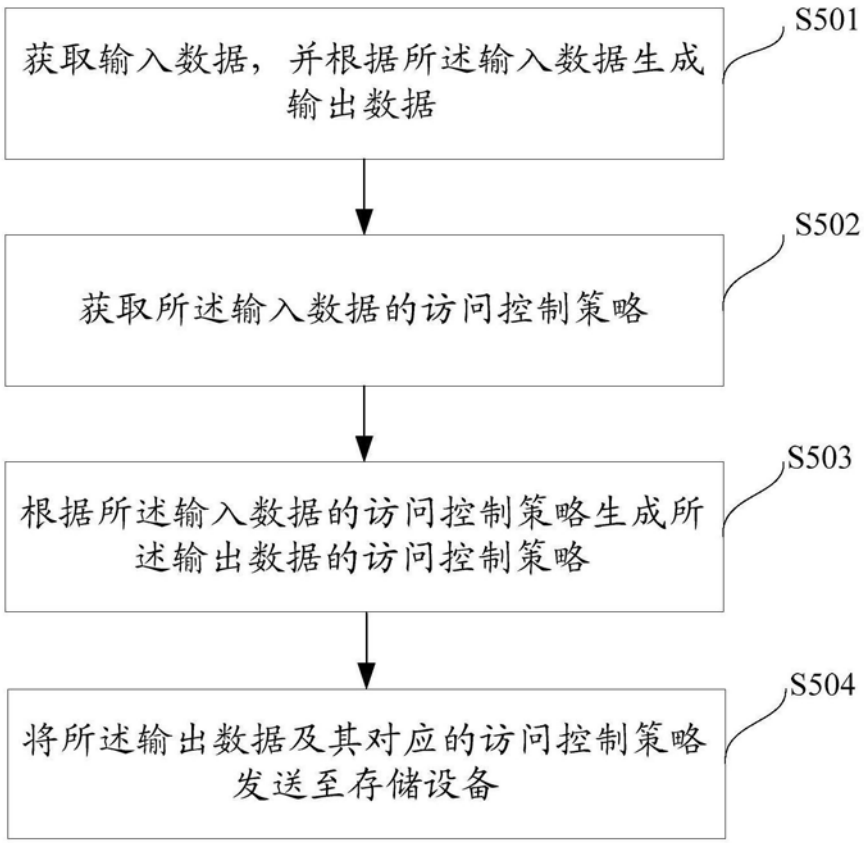

S501
获取输入数据，并根据所述输入数据生成输出数据
S502
获取所述输入数据的访问控制策略
S503
根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略
S504
将所述输出数据及其对应的访问控制策略发送至存储设备

图5

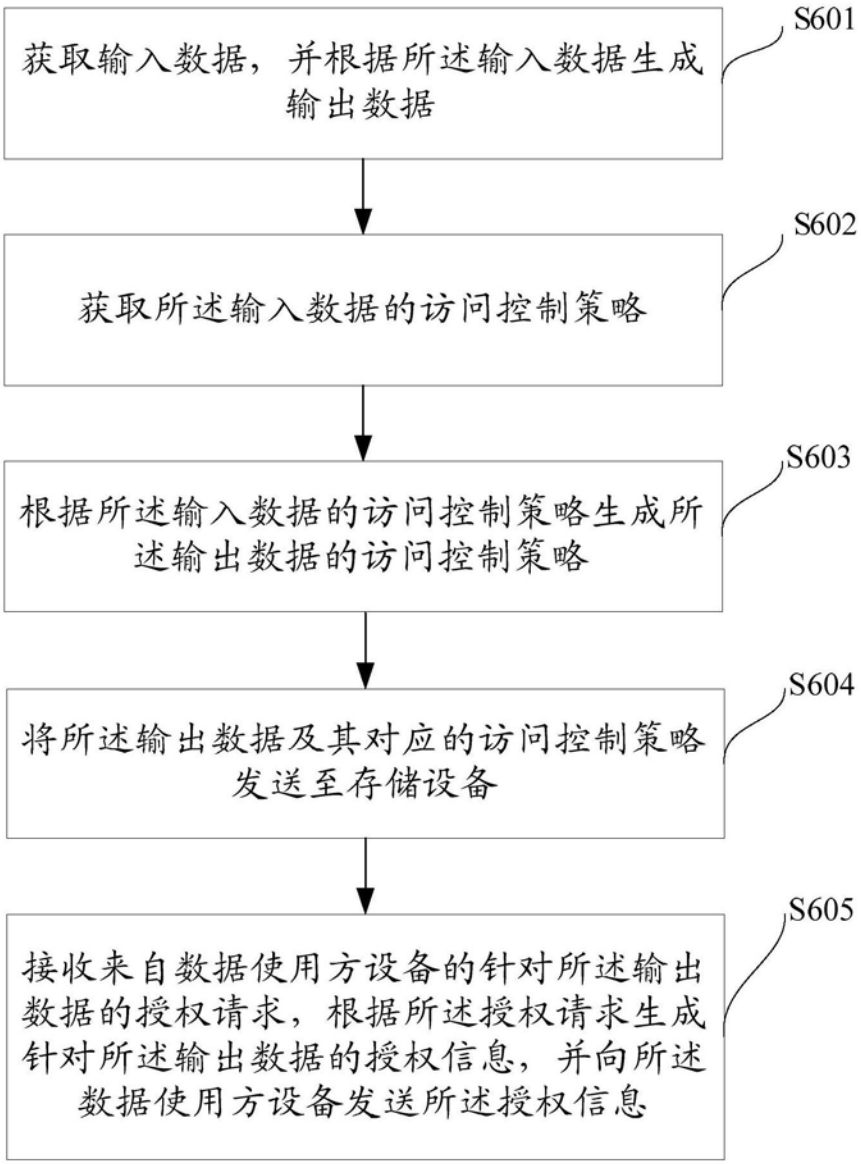

S601
获取输入数据，并根据所述输入数据生成输出数据
S602
获取所述输入数据的访问控制策略
S603
根据所述输入数据的访问控制策略生成所述输出数据的访问控制策略
S604
将所述输出数据及其对应的访问控制策略发送至存储设备
S605
接收来自数据使用方设备的针对所述输出数据的授权请求，根据所述授权请求生成针对所述输出数据的授权信息，并向所述数据使用方设备发送所述授权信息

图6

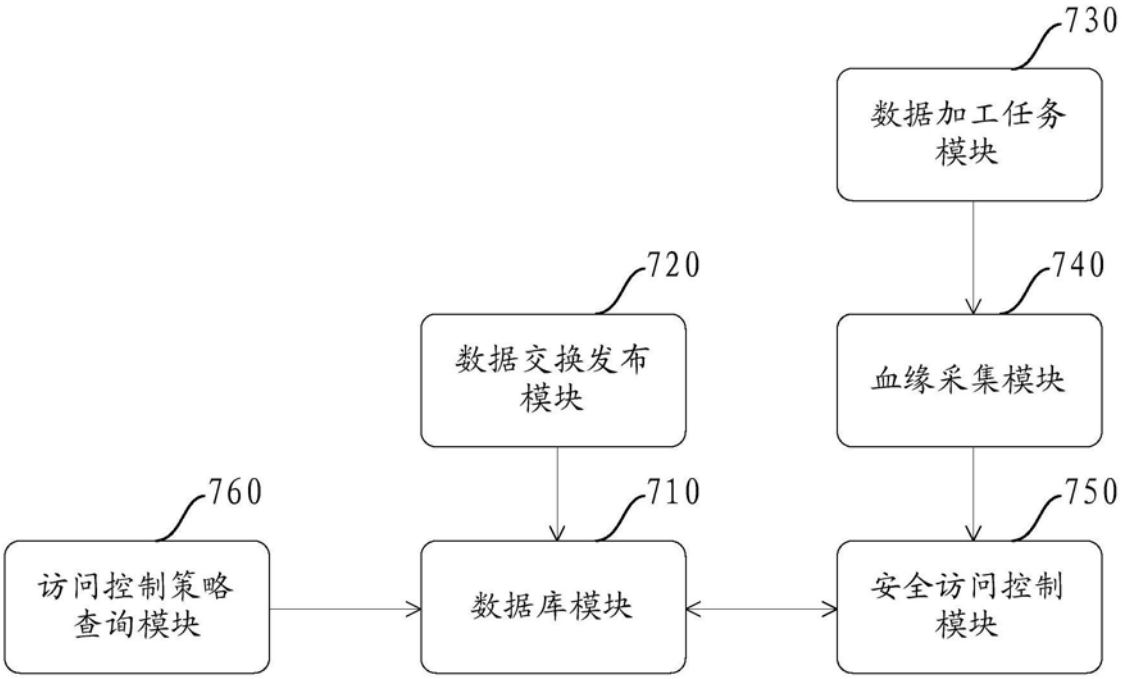

730
数据加工任务模块
720
740
数据交换发布模块
血缘采集模块
760
710
750
访问控制策略查询模块
数据库模块
安全访问控制模块

图7

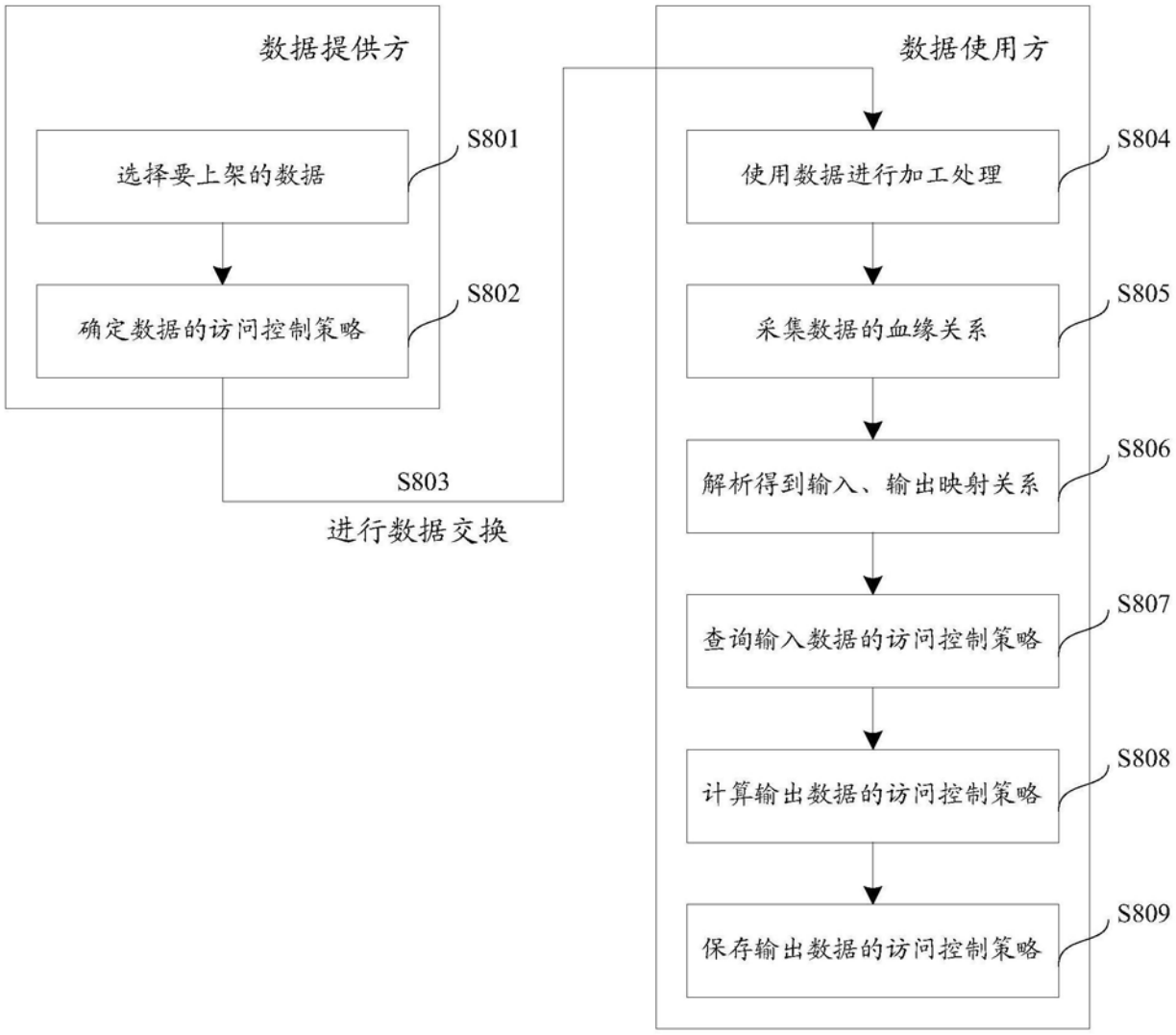

数据提供方
选择要上架的数据
S801
确定数据的访问控制策略
S802
S803
进行数据交换
数据使用方
使用数据进行加工处理
S804
采集数据的血缘关系
S805
解析得到输入、输出映射关系
S806
查询输入数据的访问控制策略
S807
计算输出数据的访问控制策略
S808
保存输出数据的访问控制策略
S809

图8