(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295367 A
(43)申请公布日 2017.01.04

(21)申请号 201610672027.4

(22)申请日 2016.08.15

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 北京奇安信科技有限公司

(72)发明人 刘敬良 黄凌志

(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生

(51)Int.Cl.
G06F 21/60(2013.01)

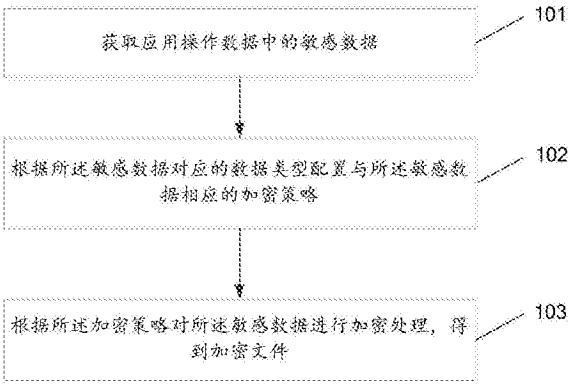
权利要求书2页 说明书10页 附图3页

(54)发明名称

数据加密方法及装置

(57)摘要

本发明公开了一种数据加密方法及装置，涉及安全技术领域，用于提高数据在云存储应用传输过程中的安全性。所述方法包括：获取应用操作中的敏感数据，根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略，根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。本发明主要用于数据的加密。



CN 106295367 A

1.一种数据加密方法，其特征在于，包括：

获取应用操作数据中的敏感数据；

根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略；

根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。

2.根据权利要求1所述的数据加密方法，其特征在于，所述获取应用操作数据中的敏感数据包括：

根据预置代理网关设备中保存的应用操作数据获取所述敏感数据。

3.根据权利要求1所述的数据加密方法，其特征在于，所述获取应用操作数据中的敏感数据包括：

从所述应用操作数据中提取与预置特征字符数据匹配的数据，得到所述应用操作数据中的敏感数据。

4.根据权利要求1所述的数据加密方法，其特征在于，所述根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略包括：

获取所述敏感数据对应的数据类型标识信息；

从预置加密策略映射表中获取与所述数据类型标识信息对应的加密策略，所述预置加密策略映射表中保存有不同数据类型标识信息分别对应的加密策略；

将所述加密策略配置为与所述敏感数据相应的加密策略。

5.根据权利要求1-4任一项所述的数据加密方法，其特征在于，所述加密策略包括密钥管理加密策略和标记化替代加密策略。

6.根据权利要求1所述的数据加密方法，其特征在于，所述方法还包括：

当接收到解密请求时，根据所述解密请求携带的标识信息对所述加密文件进行解密，所述标识信息中包含有所述加密文件的解密策略。

7.根据权利要求6所述的数据加密方法，其特征在于，所述解密策略包括密钥管理解密策略和标记化替代解密策略；

所述根据所述解密请求携带的标识信息对所述加密文件进行解密包括：

若所述标识信息包含密钥管理解密策略，则根据所述密钥管理解密策略对所述加密文件进行解密；

若所述标识信息包含标记化替代解密策略，则根据所述标记化替代解密策略对所述加密文件进行解密。

8.一种数据加密装置，其特征在于，包括：

获取单元，用于获取应用操作数据中的敏感数据；

配置单元，用于根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略；

加密单元，用于根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。

9.根据权利要求8所述的数据加密装置，其特征在于，

所述获取单元，具体用于根据预置代理网关设备中保存的应用操作数据获取所述敏感数据。

10.根据权利要求8所述的数据加密装置，其特征在于，

所述获取单元，具体还用于从所述应用操作数据中提取与预置特征字符数据匹配的数

据，得到所述应用操作数据中的敏感数据。

数据加密方法及装置

技术领域

[0001] 本发明涉及安全技术领域，特别是涉及一种数据加密方法及装置。

背景技术

[0002] 随着互联网技术的不断发展，在互联网的应用过程中，数据安全问题越来越被大家所关注。为了实现数据的保密，人们普遍采用数据加密的方式将数据妥善的保管起来。

[0003] 现有的加密服务主要通过对指定的目录和文件进行加密后存储，进而实现数据存储过程的机密性保护。然而，随着云计算时代的到来，现有的加密技术在涉及云存储应用的加密服务中，针对不同类型的数据采用相同的加密方法，使得部分数据没有被正确的加密，导致数据加密精度较低，进而导致数据在云存储应用的传输过程中安全性较低。

发明内容

[0004] 有鉴于此，本发明实施例提供一种数据加密方法及装置，能够提高数据在云存储应用传输过程中的安全性。

[0005] 为达到上述目的，本发明主要提供如下技术方案：

[0006] 一方面，本发明实施例提供了一种数据加密方法，该方法包括：

[0007] 获取应用操作数据中的敏感数据；

[0008] 根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略；

[0009] 根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。

[0010] 另一方面，本发明实施例还提供了一种数据加密装置，该装置包括：

[0011] 获取单元，用于获取应用操作数据中的敏感数据；

[0012] 配置单元，用于根据所述敏感数据对应的数据类型配置与所述敏感数 据相应的加密策略；

[0013] 加密单元，用于根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。

[0014] 本发明实施例提供的一种数据加密方法及装置，首先获取应用操作数据中的敏感数据，这里的敏感数据为能够反映用户重要信息的关键数据，然后根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略，进一步更有针对性的对不同类型数据采取不同的加密保护策略，防止敏感数据被窃取，最后根据所述加密策略对所述敏感数据进行加密处理，与现有技术中云存储应用中采用相同的加密方法相比，本发明通过对不同数据类型的敏感数据采用不同的加密策略，使得不同数据类型的数据能够被正确的加密，提高了加密精度，更有效的防止用户的敏感数据泄露，进一步提高了数据在云存储应用的传输过程中的安全性。

[0015] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0016] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0017] 图1示出了本发明实施例提供的一种数据加密方法流程图；

[0018] 图2示出了本发明实施例提供的另一种数据加密方法流程图；

[0019] 图3示出了本发明实施例提供的一种数据加密装置结构示意图；

[0020] 图4示出了本发明实施例提供的另一种数据加密装置结构示意图。

具体实施方式

[0021] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开 而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0022] 本发明实施例提供一种数据加密方法，如图1所示，所述方法包括：

[0023] 101、获取应用操作数据中的敏感数据。

[0024] 这里的敏感数据为对于用户或者企业具有重要意义的关键数据，例如账号密码、联系方式、银行卡号或者企业中涉及商业机密的重要数据等，本发明实施例对敏感信息的类型不做限定，具体可根据用户实际需求在上传数据之前在客户端进行预先设置。

[0025] 这里的应用操作数据中可以包括但不局限于用于http协议在交互过程中产生的应用操作数据，如在进行数据移动、删除、复制、回收和共享等操作产生的数据，本发明实施例对应用操作数据的类型不做限定，可根据实际应用中进行选取。

[0026] 对于本发明实施例，当用户使用云服务器进行数据的获取或者数据的上传的同时，首先通过预置代理网关设备中获取应用操作数据，这里的预置代理网关设备是代理服务器的一种，它能够根据用户携带的域名登陆自己的代理网关，进而建立数据连接，将待处理的数据的上传至代理网管，根据代理网关实现数据的转发，从而上传至云服务器，以便云服务器为用户构建更稳定、更安全的应用，然后根据应用操作数据中的特征字符数据识别出应用操作数据中的敏感数据，进而获取敏感数据。

[0027] 102、根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略。

[0028] 本发明实施例中的数据类型主要分为动态数据和静态数据，静态数据主要指的是当用户在查看数据时已生成，并没有与服务器数据库进行交互的数据，主要指硬盘、存储空间中的数据等，动态数据主要指在系统应用中随时间变化而改变的数据，与服务器数据库有交互的数据，如用户访问的数据、流量数据等。

[0029] 由于不同数据类型的敏感数据的稳定性有所不同，本发明实施例针对不同数据类型的敏感数据采用不同的加密策略，这里的加密策略主要包括 密钥管理加密策略和标记化替代加密策略，举例来说，若识别出所述敏感数据为身份证号数据，则配置与身份证号数据相应的加密策略，若识别出所述敏感数据为利用标记化替代加密策略将身份证号中的某几位数字采用特殊的标识进行替代，并且将加密后的数据与原始数据保存至本地数据库。

[0030] 上述的密钥管理是现有云服务提供商可以提供的基于加密密钥方案来保护用户的数据，具体可以包括保护密钥存储，使得数据在存储、传输和备份中都受到保护，还可以包括访问密钥存储，限制只有特定需要单独密钥的实体可以访问密钥存储，还可以包括密钥的备份和恢复，以便更好的保护数据；

[0031] 上述的标记化替代是通过将敏感数据采用标记化字符进行替代从而实现加密处理，避免敏感数据被泄露的风险，本发明实施例对这里的标记化替代字符的形式不做限定，具体可以根据实际需求进行选取。

[0032] 103、根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。

[0033] 本步骤中，需要说明的是，本发明实施例对不同数据类型的敏感数据所采用的机密策略不做限定，具体可根据用户实际需求进行合理选取。

[0034] 对于本发明实施例，具体的应用场景可以如下所示，但不限于此，包括：当预置网关设备接收到应用操作数据后，获取应用操作数据中的涉及用户隐私的敏感关键词，具体包括用户的名字、身份信息和联系方式等设计隐私的数据，进一步识别该敏感关键词对应的数据类型，则根据该敏感关键词所对应的数据类型配置与该敏感关键词相应的标记化替换加密策略，将该关键词替换为星形的标记，进而对该敏感关键词进行加密处理，得到加密密文，使得在数据传输和上传的过程中他人无法查看该敏感关键词，进一步实现对敏感数据的保护。

[0035] 本发明实施例提供的一种数据加密方法，首先获取应用操作数据中的敏感数据，这里的敏感数据为能够反映用户重要信息的关键数据，然后根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略，进一步更有针对性的对不同类型数据采取不同的加密保护策略，防止敏感数据被窃取，最后根据所述加密策略对所述敏感数据进行加密处理，与现有 技术中云存储应用中采用相同的加密方法相比，本发明通过对不同数据类型的敏感数据采用不同的加密策略，提高了加密精度，使得不同数据类型的数据能够被正确的加密，更有效的防止用户的敏感数据泄露，进一步提高了数据在云存储应用的传输过程中的安全性。

[0036] 进一步地，本发明实施例提供另一种数据加密方法，如图2所示，所述方法包括：

[0037] 201、根据预置代理网关设备中保存的应用操作数据获取敏感数据。

[0038] 其中，预置代理网关设备是在传输层上实现网络连接的设备，它能够将用户待处理的数据与云服务器之间建立连接，从而实现合法的数据转发，进行对转发数据进行控制和登记，保证转发数据的安全可靠性。

[0039] 具体地，对预置代理设备中保存的应用操作数据进行特征提取，将提取与预置特征字符数据匹配的数据作为敏感数据，这里的应用操作数据中可以包括但不局限于用于http协议在交互过程中产生的应用操作数据，如在进行数据移动、删除、复制、回收和共享等操作产生的数据。

[0040] 示例性的，用户在上传数据至云服务器进行数据保存的过程中，首先将该待保存的数据传输至预置代理设备中，获取待保存数据中的交互动作产生的数据，进一步提取交互动作产生的数据中与预置敏感字符数据相匹配的敏感关键词，得到待保存数据中的敏感数据，以便对敏感数据进行加密。

[0041] 上述的预置敏感字符数据可以包括但不限制于用户的账户信息、身份信息和机密

文件等字符数据，本发明实施例对预置敏感字符数据不做限定，这里的预置敏感字符数据根据用户需求可以相应配置，以便根据用户需求进行保密设置。

[0042] 202、获取所述敏感数据对应的数据类型标识信息。

[0043] 由于不同应用场景下的操作产生的数据类型标识有所不同，本发明实施例敏感数据的数据类型的不同采取不同的加密方式。这里的数据类型可以分为两大类，静态数据和动态数据，另外也可以具体将每个大分类划分为多个子分类，如日期型数据、字符型数据和逻辑型数据等。

[0044] 这里的数据类型标识信息为携带有能够识别数据类型的信息，具体的 数据类型可以根据时间情况进行划分，进一步根据划分的数据类型选取合适的标识信息作为判断数据类型的依据，本发明实施例对所述数据类型标识信息所包含的特征不做限定，具体可根据实际情况进行选取。

[0045] 203、从预置加密策略映射表中获取与所述数据类型标识信息对应的加密策略。

[0046] 当获取到应用操作数据中的敏感数据后，根据查找预置加密策略映射表，获取与敏感数据类型对应的加密策略，进一步对不同数据类型做不同的加密处理，这里的预置加密策略映射表中保存有不同数据类型标识信息分别对应的加密策略，如对于一些交互性较强的数据可以采用标记化替代加密策略，如下表1所示，该表中保存有对应采用标记化加密策略的多种数据及该数据对应的标号，另外，对于其他类型的数据可采用密钥管理加密策略，需要说明的是，本发明实施例对预置加密策略映射表中不同数据类型对应的加密策略不做限定。

[0047] 表1加密策略映射表

[0048]

标号	数据类型	加密策略
30000	电话号码	标记化替代加密策略
30001	电子邮件	标记化替代加密策略
30002	日期	标记化替代加密策略
30003	身份证号	标记化替代加密策略
30004	数字	标记化替代加密策略
30005	URL	标记化替代加密策略
30006	电子邮件	标记化替代加密策略
30007	日期	标记化替代加密策略
30008	可搜索及排序	标记化替代加密策略
30009	字段	标记化替代加密策略
30010	姓名	标记化替代加密策略

[0049] 204、将所述加密策略配置为与所述敏感数据相应的加密策略。

[0050] 由于不同应用场景下的操作产生的数据类型有所不同，本发明实施例 敏感数据的数据类型的不同采取不同的加密方式，对于磁盘上静态数据或者生产数据库中的静态数据的加密尤为重要，因为这样可以用来防止恶意的云服务提供商、恶意的邻居“租户”及某些类型应用的滥用。这些用户控制并保存密钥，在自己需要的情况下解密数据。

[0051] 相应地，对于加密传输中的动态数据，如信用卡号、密码和私钥等，虽然云提供商

网络可能比开放网络安全，但是他们使用其特有的、由许多不同的组成部分构成的架构，且由不同的组织共享云。因此，即便实在云提供商的网络中，保护这些传输中的敏感数据和受监管信息也是非常重要的。

[0052] 需要说明的是，由于动态数据的结构不确定总的数据存储量，而是现有的每一个数据元素定义一个确定的初始大小的空间，若干个数据元素分配若干个同样大小的空间，当数据发生变化时，数据的存储空间也会发生变化，因此动态数据相对不固定，由于标记化替代的加密策略对当前加密的敏感数据的随机性比较，并且不会配置有相应的解密密钥，需要在原始加密处进行标记化解密，才能获取解密文件，因此对于时常变化的动态数据采用的标记化替代的加密策略，更能够保证数据的安全性。

[0053] 205、根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。

[0054] 根据步骤203中的预置加密策略表中查找到对应的加密策略对敏感数据进行加密，本发明实施例中的加密策略主要包括密钥管理加密策略和标记化替代加密策略。

[0055] 进一步对上述的密钥管理加密策略和标记化替代加密策略进行说明，密钥管理加密策略主要通过对敏感数据生成加密密钥，进而避免攻击者访问敏感数据，标记化替代加密策略主要通过将敏感数据的全部或者涉及数字类的字符采用特殊的标记符号进行替代，从而进行加密。

[0056] 206、当接收到解密请求时，根据所述解密请求携带的标识信息对所述加密文件进行解密。

[0057] 本步骤中，其中，所述标识信息中包含有所述加密文件的解密策略，解密策略与上述的加密策略相对应，包括密钥管理解密策略和标记化替代解密秘钥，若所述标识信息包含密钥管理解密策略，则根据所述密钥管理 解密策略对所述加密文件进行解密，若所述标识信息包含标记化替代解密策略，则根据所述标记化替代解密策略对所述加密文件进行解密。

[0058] 需要说明的是，这里的密钥管理解密策略与密钥管理加密策略相对应，是一种参数，它是根据密钥管理加密策略反向对应生成的解密密钥；相应地，标记化替代解密策略与标记化替代加密策略相对应，它是根据标记化替代加密策略对应的解密密钥，从而将加密文件中所标记的敏感数据还原为加密前的原始数据。

[0059] 对于本发明实施例，具体的应用场景可以如下所示，但不限于此，包括：当前的应用场景为用户从云端服务器下载已上传的数据并且对该数据进行解密的过程，首先云服务器将待处理数据传输并保存至与用户登陆信息相匹配的代理网关设备，然后从代理网关设备中保存的待处理数据中获取已经被加密的敏感数据，此时针对敏感数据加密时采用的不同加密策略，在进行敏感数据解密时也有相应的解密策略，若加密文件的数据为硬盘存储数据，通常查找在预置代理网关设备查找到该加密数据对应的密钥管理解密策略，进一步根据密钥管理解密策略对已被加密的文件进行解密，进一步还原得到原始的敏感数据。

[0060] 本发明实施例的另一种数据加密方法，通过预置网关代理设备对转发数据进行控制和处理，一方面保证了转发数据的安全可靠性，另外一方面对用户登陆进行限制，防止恶意用户的攻击，进一步对不同数据类型应用操作数据中的敏感数据采用不同的加密策略和解密策略，在提高数据加密精度的同时保证了敏感数据在数据上传和下载过程中的安全性。

[0061] 进一步地，作为图1所示方法的具体实现，本发明实施例提供一种数据加密装置，如图3所示，所述装置可以包括：获取单元31、配置单元32、加密单元33。

[0062] 所述获取单元31，用于获取应用操作数据中的敏感数据，其中，敏感数据为对于用户或者企业具有重要意义的关键数据，具体可通过预置代理网关设备中的应用操作数据获取敏感数据；

[0063] 所述配置单元32，用于根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略，其中，加密策略可以包括密钥管理加密策略和 标记化替代加密策略；

[0064] 所述加密单元33，用于根据所述加密策略对所述敏感数据进行加密处理，得到加密文件。

[0065] 需要说明的是，本发明实施例提供的一种数据加密装置所涉及各功能单元的其他相应描述，可以参考图1所示方法中的对应描述，在此不再赘述。

[0066] 本发明实施例提供的一种数据加密装置，首先获取应用操作数据中的敏感数据，这里的敏感数据为能够反映用户重要信息的关键数据，然后根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略，进一步更有针对性的对不同类型数据采取不同的加密保护策略，防止敏感数据被窃取，最后根据所述加密策略对所述敏感数据进行加密处理，与现有技术中云存储应用中采用相同的加密方法相比，本发明通过对不同数据类型的敏感数据采用不同的加密策略，提高了加密精度，使得不同数据类型的数据能够被正确的加密，更有效的防止用户的敏感数据泄露，进一步提高了数据在云存储应用的传输过程中的安全性。

[0067] 进一步地，作为图2所示方法的具体实现，本发明实施例提供另一种数据加密装置，如图4所示，所述装置可以包括：获取单元41、配置单元42、加密单元43、解密单元44，

[0068] 所述获取单元41，用于获取应用操作数据中的敏感数据，其中，敏感数据为对于用户或者企业具有重要意义的关键数据，具体可通过预置代理网关设备中的应用操作数据获取敏感数据；

[0069] 所述配置单元42，用于根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略，其中，加密策略可以包括密钥管理加密策略和标记化替代加密策略；

[0070] 所述加密单元43，用于根据所述加密策略对所述敏感数据进行加密处理，得到加密文件；

[0071] 所述解密单元44，用于当接收到解密请求时，根据所述解密请求携带的标识信息对所述加密文件进行解密，所述标识信息中包含有所述加密文件的解密策略，其中，解密策略可以包括密钥管理解密策略和标记化替代 解密策略。

[0072] 进一步地，所述解密单元44包括：

[0073] 第一解密模块4401，用于若所述标识信息包含密钥管理解密策略，则根据所述密钥管理解密策略对所述加密文件进行解密；

[0074] 第二解密模块4402，用于若所述标识信息包含标记化替代解密策略，则根据所述标记化替代解密策略对所述加密文件进行解密。

[0075] 进一步地，所述获取单元41，具体用于根据预置代理网关设备中保存的应用操作数据获取所述敏感数据；

[0076] 进一步地，所述获取单元41，具体还用于从所述应用操作数据中提取与预置特征

字符数据匹配的数据，得到所述应用操作数据中的敏感数据。

[0077] 进一步地，所述配置单元42包括：

[0078] 第一获取模块4201，用于获取所述敏感数据对应的数据类型标识信息；

[0079] 第二获取模块4202，用于从预置加密策略映射表中获取与所述数据类型标识信息对应的加密策略，所述预置加密策略映射表中保存有不同数据类型标识信息分别对应的加密策略；

[0080] 配置模块4203，用于将所述加密策略配置为与所述敏感数据相应的加密策略。

[0081] 需要说明的是，本发明实施例提供的另一种数据加密装置所涉及各功能单元的其他相应描述，可以参考图2所示方法中的对应描述，在此不再赘述。

[0082] 本发明实施例的另一种数据加密装置，通过预置网关代理设备对转发数据进行控制和处理，一方面保证了转发数据的安全可靠性，另外一方面对用户登陆进行限制，防止恶意用户的攻击，进一步对不同数据类型应用操作数据中的敏感数据采用不同的加密策略和解密策略，在提高数据加密精度的同时保证了敏感数据在数据上传和下载过程中的安全性。

[0083] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0084] 可以理解的是，上述方法及装置中的相关特征可以相互参考。另外，上述实施例中的“第一”、“第二”等是用于区分各实施例，而并不代表各实施 例的优劣。

[0085] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0086] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0087] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0088] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0089] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何

组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述,本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0090] 此外,本领域的技术人员能够理解,尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征,但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如,在下面的权利要求书中,所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0091] 本发明的各个部件实施例可以以硬件实现,或者以在一个或者多个处理器上运行的软件模块实现,或者以它们的组合实现。本领域的技术人员应当理解,可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的一种数据存储的方法及装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如,计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上,或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到,或者在载体信号上提供,或者以任何其他形式提供。

[0092] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制,并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中,不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中,这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0093] 本发明实施例还公开了,A1、一种数据加密方法,包括:

[0094] 获取应用操作数据中的敏感数据;

[0095] 根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略;

[0096] 根据所述加密策略对所述敏感数据进行加密处理,得到加密文件。

[0097] A2、根据A1所述的方法,所述获取应用操作数据中的敏感数据包括:根据预置代理网关设备中保存的应用操作数据获取所述敏感数据。

[0098] A3、根据A1所述的方法,所述获取应用操作数据中的敏感数据包括:

[0099] 从所述应用操作数据中提取与预置特征字符数据匹配的数据,得到所述应用操作数据中的敏感数据。

[0100] A4、根据A1所述的方法,所述根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略包括:

[0101] 获取所述敏感数据对应的数据类型标识信息;

[0102] 从预置加密策略映射表中获取与所述数据类型标识信息对应的加密策略,所述预置加密策略映射表中保存有不同数据类型标识信息分别对应的加密策略;

[0103] 将所述加密策略配置为与所述敏感数据相应的加密策略。

[0104] A5、根据权利要求A1-A4中任一项所述的方法，所述加密策略包括密钥管理加密策略和标记化替代加密策略。

[0105] A6、根据A1所述的方法，所述方法还包括：

[0106] 当接收到解密请求时，根据所述解密请求携带的标识信息对所述加密文件进行解密，所述标识信息中包含有所述加密文件的解密策略。

[0107] A7、根据A6所述的方法，所述解密策略包括密钥管理解密策略和标记化替代解密策略；

[0108] 所述根据所述解密请求携带的标识信息对所述加密文件进行解密包括：

[0109] 若所述标识信息包含密钥管理解密策略，则根据所述密钥管理解密策略对所述加密文件进行解密；

[0110] 若所述标识信息包含标记化替代解密策略，则根据所述标记化替代解密策略对所述加密文件进行解密。

[0111] B8、一种数据加密装置，包括：

[0112] 获取单元，用于获取应用操作数据中的敏感数据；

[0113] 配置单元，用于根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略；

[0114] 加密单元，用于根据所述加密策略对所述敏感数据进行加密处理，得 到加密文件。

[0115] B9、根据B8所述的装置，所述获取单元，具体用于根据预置代理网关设备中保存的应用操作数据获取所述敏感数据。

[0116] B10、根据B8所述的装置，所述获取单元，具体还用于从所述应用操作数据中提取与预置特征字符数据匹配的数据，得到所述应用操作数据中的敏感数据。

[0117] B11、根据B8所述的装置，所述配置单元包括：

[0118] 第一获取模块，用于获取所述敏感数据对应的数据类型标识信息；

[0119] 第二获取模块，用于从预置加密策略映射表中获取与所述数据类型标识信息对应的加密策略，所述预置加密策略映射表中保存有不同数据类型标识信息分别对应的加密策略；

[0120] 配置模块，用于将所述加密策略配置为与所述敏感数据相应的加密策略。

[0121] B12、根据B8-B11中任一项所述的装置，所述加密策略包括密钥管理加密策略和标记化替代加密策略。

[0122] B13、根据B8所述的装置，所述装置还包括：

[0123] 解密单元，用于当接收到解密请求时，根据所述解密请求携带的标识信息对所述加密文件进行解密，所述标识信息中包含有所述加密文件的解密策略。

[0124] B14、根据B8所述的装置，所述解密策略包括密钥管理解密策略和标记化替代解密策略；

[0125] 所述解密单元包括：

[0126] 第一解密模块，用于若所述标识信息包含密钥管理解密策略，则根据所述密钥管理解密策略对所述加密文件进行解密；

[0127] 第二解密模块，用于若所述标识信息包含标记化替代解密策略，则根据所述标记

化替代解密策略对所述加密文件进行解密。

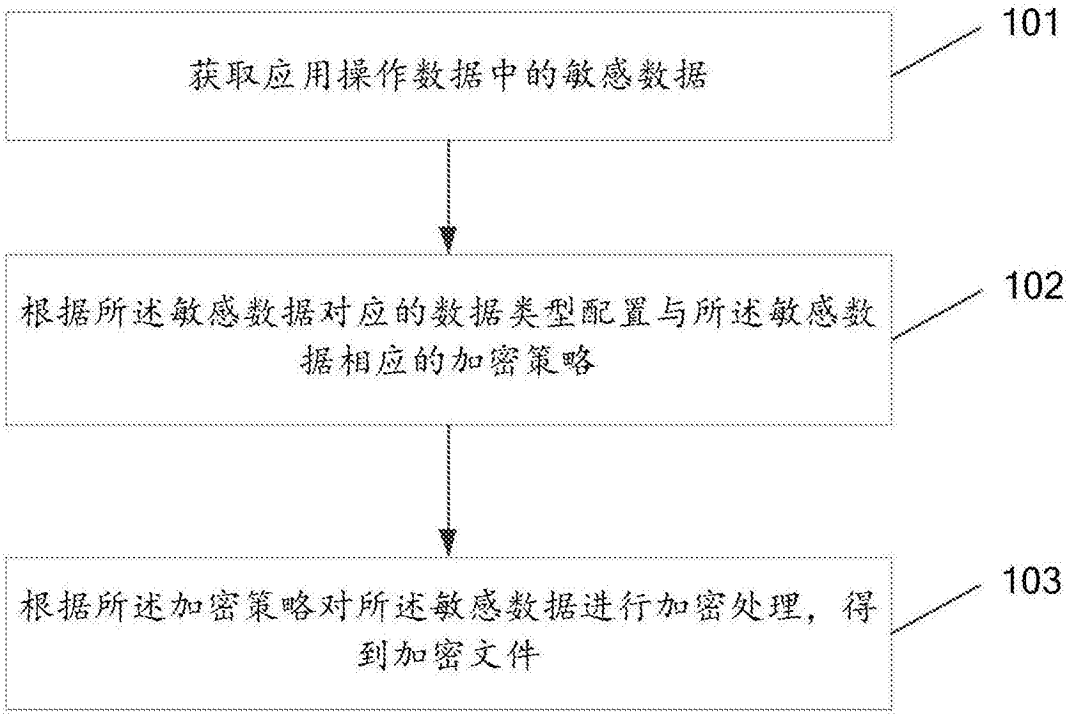

获取应用操作数据中的敏感数据
101
根据所述敏感数据对应的数据类型配置与所述敏感数据相应的加密策略
102
根据所述加密策略对所述敏感数据进行加密处理，得到加密文件
103

图1

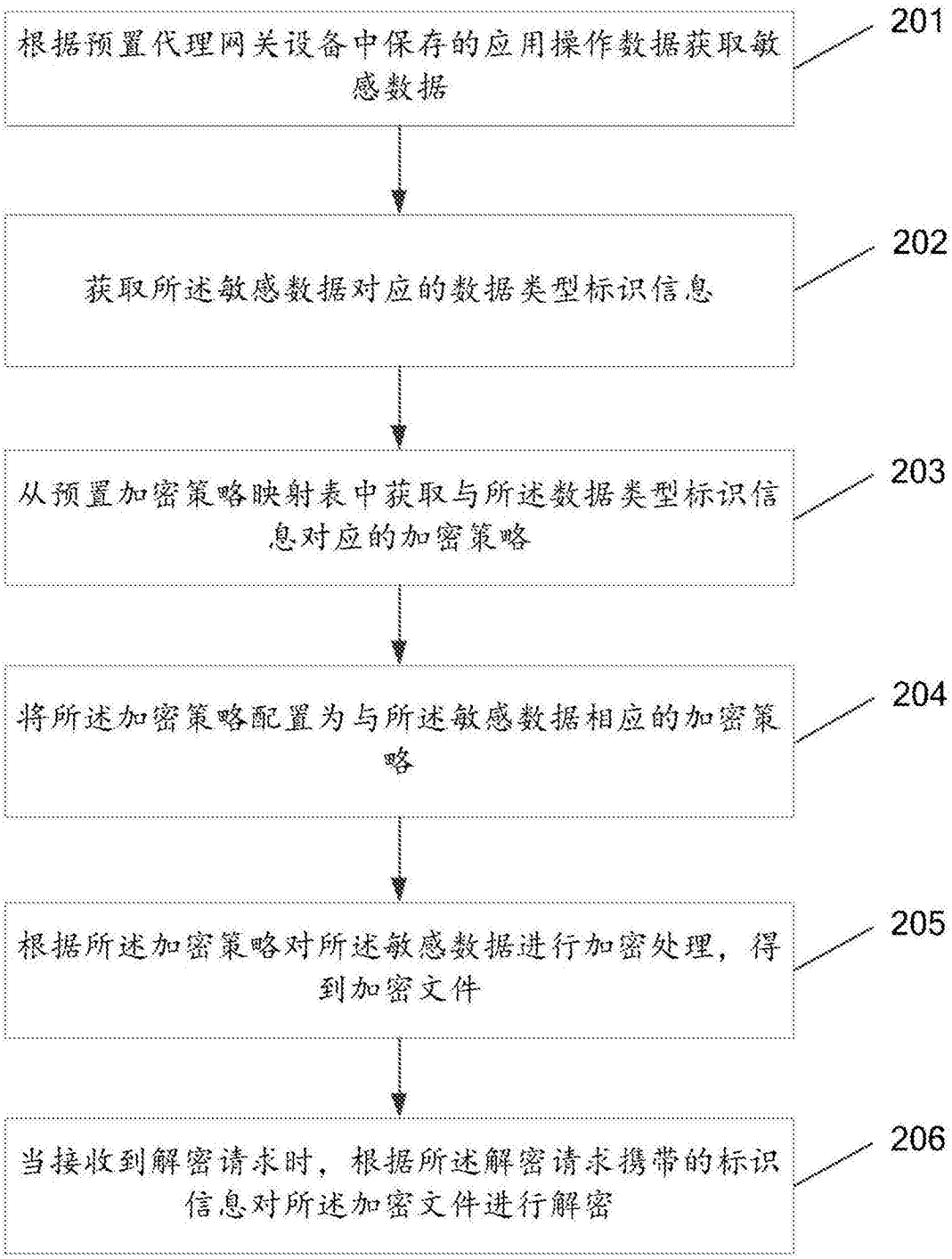

根据预置代理网关设备中保存的应用操作数据获取敏感数据
201
获取所述敏感数据对应的数据类型标识信息
202
从预置加密策略映射表中获取与所述数据类型标识信息对应的加密策略
203
将所述加密策略配置为与所述敏感数据相应的加密策略
204
根据所述加密策略对所述敏感数据进行加密处理，得到加密文件
205
当接收到解密请求时，根据所述解密请求携带的标识信息对所述加密文件进行解密
206

图2

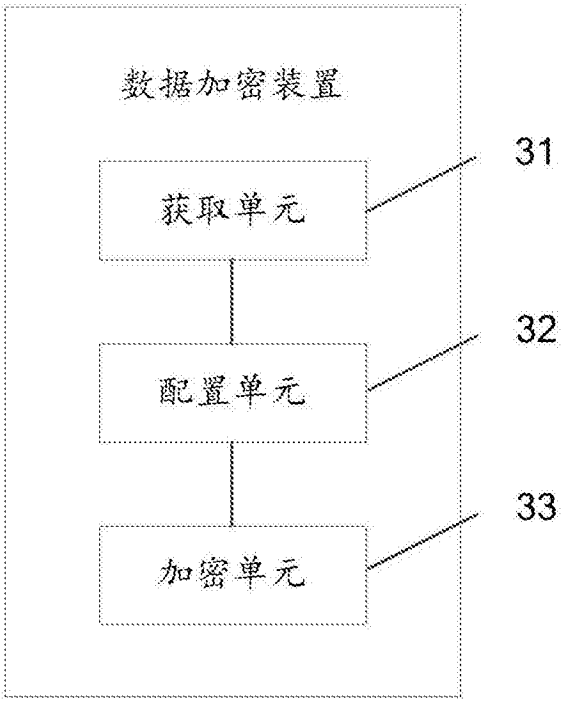

数据加密装置
获取单元
31
配置单元
32
加密单元
33

图3

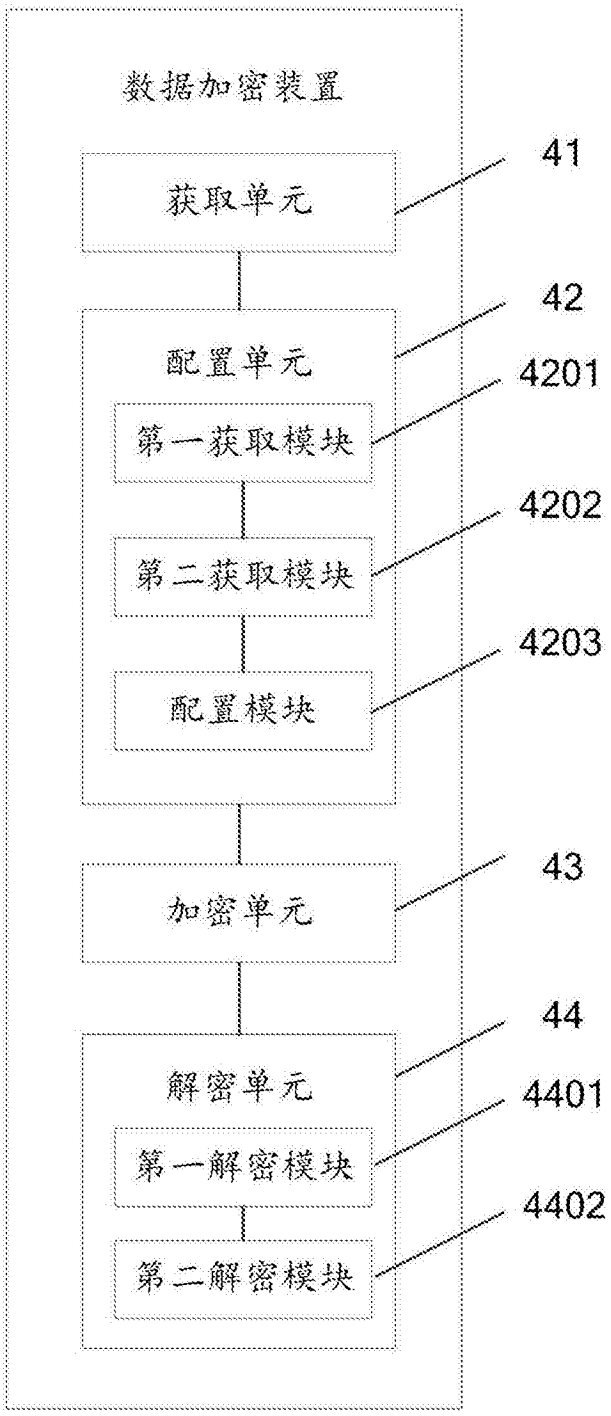

数据加密装置
获取单元
41
配置单元
42
第一获取模块
4201
第二获取模块
4202
配置模块
4203
加密单元
43
解密单元
44
第一解密模块
4401
第二解密模块
4402

图4