

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 1 月 24 日 (24.01.2019)



(10) 国际公布号
WO 2019/015598 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2018/096072

(22) 国际申请日: 2018 年 7 月 18 日 (18.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710591062.8 2017 年 7 月 19 日 (19.07.2017) CN

(71) 申请人: 腾讯科技(深圳)有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。

(72) 发明人: 孙彬(SUN, Bin); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。 王建(WANG, Jian); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。 李杰(LI, Jie); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。 吴先斌(WU, Xianbin); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。 屈宇鹏(QU, Yupeng); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。 位爱伶(WEI, Ailing); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。 蔡舒(CAI, Shu); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。

(54) Title: HYBRID-CLOUD DATA STORAGE METHOD AND APPARATUS, RELATED DEVICE, AND CLOUD SYSTEM

(54) 发明名称: 混合云的数据存储方法、装置、相关设备及云系统

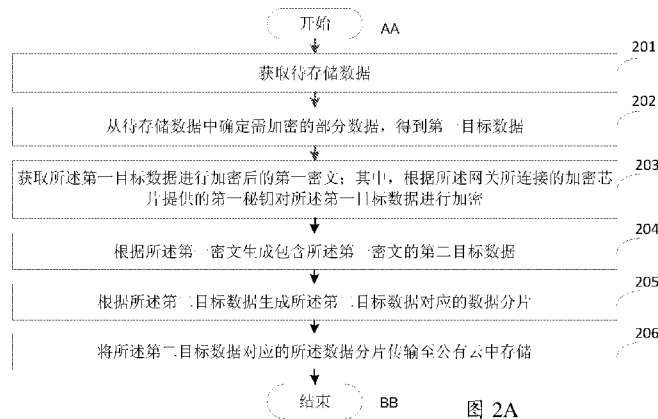


图 2A

201 OBTAIN DATA TO BE STORED
202 DETERMINE A PART OF DATA NEEDING TO BE ENCRYPTED FROM THE DATA TO BE STORED, SO AS TO OBTAIN FIRST TARGET DATA
203 ACQUIRE A FIRST CRYPTOGRAPH AFTER THE FIRST TARGET DATA IS ENCRYPTED, WHEREIN THE FIRST TARGET DATA IS ENCRYPTED BY USING A FIRST SECRET KEY PROVIDED BY AN ENCRYPTION CHIP CONNECTED TO THE GATEWAY
204 GENERATE SECOND TARGET DATA CONTAINING THE FIRST CRYPTOGRAPH ACCORDING TO THE FIRST CRYPTOGRAPH
205 GENERATE A DATA FRAGMENT CORRESPONDING TO THE SECOND TARGET DATA ACCORDING TO THE SECOND TARGET DATA
206 TRANSMIT THE DATA FRAGMENT CORRESPONDING TO THE SECOND TARGET DATA TO A PUBLIC CLOUD FOR STORAGE
AA START
BB END

(57) Abstract: Embodiments of the present application provide a hybrid-cloud data storage method and apparatus, a related device, and a cloud system. The hybrid-cloud data storage method comprises: a gateway of a private cloud obtains data to be stored; determine a part of data needing to be encrypted from the data to be stored, so as to obtain first target data; acquiring a first cryptograph after the first target data is encrypted, wherein the first target data is encrypted by using a first secret key provided by an encryption chip connected to the gateway; generate second target data containing the first cryptograph according to the first cryptograph; generate a

(CN)。 龚幽兰(GONG, Youlan); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 王利虎(WANG, Lihu); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(74) 代理人: 北京德琦知识产权代理有限公司(DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区知春路1号学院国际大厦7层, Beijing 100083 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

data fragment corresponding to the second target data according to the second target data; and transmit the data fragment corresponding to the second target data to a public cloud for storage.

(57) 摘要: 本申请实施例提供一种混合云的数据存储方法、装置、相关设备及云系统, 其中数据存储方法包括: 私有云的网关获取待存储数据; 从待存储数据中确定需加密的部分数据, 得到第一目标数据; 获取所述第一目标数据进行加密后的第一密文; 其中, 根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密; 根据所述第一密文生成包含所述第一密文的第二目标数据; 根据所述第二目标数据生成第二目标数据对应的数据分片; 将第二目标数据对应的所述数据分片传输至公有云中存储。

混合云的数据存储方法、装置、相关设备及云系统

本申请要求于2017年07月19日提交中国专利局、申请号为201710591062.8、名称为“混合云的数据存储方法、装置、相关设备及云系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本申请涉及数据处理技术领域，具体涉及一种混合云的数据存储方法、装置、相关设备及云系统。

背景

- 10 混合云是指公有云和私有云的组合，已成为云计算的主要模式和发展方向之一。其中，公有云是由公有云服务提供商提供的计算资源，可供所有的网络用户使用，是可由所有企业和用户共享使用的云环境；私有云是出于安全性考虑的一种由特定用户专享的云环境，如针对某一企业搭建的私有云，私有云中的资源仅供该企业的内部用户，或者与该企业相关的特定外部用户使用。

技术内容

- 15 本申请实施例提供了一种混合云的数据存储方法，应用于私有云的网关，所述方法包括：
- 获取待存储数据；
- 从待存储数据中确定需加密的部分数据，得到第一目标数据；
- 获取所述第一目标数据进行加密后的第一密文；其中，根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密；
- 20 根据所述第一密文生成包含所述第一密文的第二目标数据；
- 根据所述第二目标数据生成所述第二目标数据对应的数据分片；
- 将所述第二目标数据对应的所述数据分片传输至公有云中存储。
- 本申请实施例还提供一种混合云的数据读取方法，应用于私有云的网关，所述方法包括：
- 25 获取公有云中的存储数据；所述存储数据包括至少一个数据分片，所述至少一个数据分片包括需读取的数据块，和该数据块相应的元数据；
- 对所述存储数据中的各数据分片进行逐片解压，如果解压过程中，确定数据分片中存在加密的数据块，根据该数据块的元数据选取解密算法，及确定网关连接的加密芯片提供的密钥；
- 30 根据所述解密算法和密钥，对数据分片中存在加密的数据块进行解密；
- 将数据分片解压后的未加密的数据块，和数据分片中解密的数据块相合并，得到读取数据；
- 反馈所述读取数据给终端设备。

本申请实施例还提供一种混合云的数据存储装置，包括：存储器、处理器；其中，所述存储器中存储有计算机可读指令，所述处理器执行所述存储中的计算机可读指令，用于：

获取待存储数据；

5 从待存储数据中确定需加密的部分数据，得到第一目标数据；

获取所述第一目标数据进行加密后的第一密文；其中，根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密；

根据所述第一密文生成包含所述第一密文的第二目标数据；

根据所述第二目标数据生成所述第二目标数据对应的数据分片；

10 将第二目标数据对应的所述数据分片传输至公有云中存储。本申请实施例还提供一种网关，包括：存储器和处理器，所述存储器存储有程序，所述处理器调用所述程序；所述程序用于：

获取待存储数据；

从待存储数据中确定需加密的部分数据，得到第一目标数据；

15 获取所述第一目标数据进行加密后的第一密文；其中，根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密；

根据所述第一密文生成包含所述第一密文的第二目标数据；

根据所述第二目标数据生成所述第二目标数据对应的数据分片；

将所述第二目标数据对应的所述数据分片传输至公有云中存储。

20 本申请实施例还提供一种存储介质，所述存储介质记录有程序，所述程序用于：

获取待存储数据；

从待存储数据中确定需加密的部分数据，得到第一目标数据；

25 获取所述第一目标数据进行加密后的第一密文；其中，根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密；

根据所述第一密文生成包含所述第一密文的第二目标数据；

根据所述第二目标数据生成所述第二目标数据对应的数据分片；

将所述第二目标数据对应的所述数据分片传输至公有云中存储。

30 本申请实施例还提供一种混合云的数据读取装置，包括：存储器、处理器；其中，所述存储器中存储有计算机可读指令，所述处理器执行所述存储中的计算机可读指令，用于：

获取公有云中的存储数据；所述存储数据包括至少一个数据分片，所述至少一个数据分片包括需读取的数据块，和该数据块相应的元数据；

35 对所述存储数据中的各数据分片进行逐片解压，如果解压过程中，确定数据分片中存在加密的数据块，根据该数据块的元数据选取解密算法，及确定网关连接的加密芯片提供的密钥；

根据所述解密算法和密钥，对数据分片中存在加密的数据块进行解密；

将数据分片解压后的未加密的数据块，和数据分片中解密的数据块相合并，得到读取数据；

40 反馈所述读取数据给终端设备。

本申请实施例还提供一种网关，包括：存储器和处理器，所述存储器存储有程序，所述处理器调用所述程序；所述程序用于：

获取公有云中的存储数据；所述存储数据包括至少一个数据分片，所述至少

一个数据分片包括需读取的数据块, 和该数据块相应的元数据;

对所述存储数据中的各数据分片进行逐片解压, 如果解压过程中, 确定数据分片中存在加密的数据块, 根据该数据块的元数据选取解密算法, 及确定网关连接的加密芯片提供的密钥;

5 根据所述解密算法和密钥, 对数据分片中存在加密的数据块进行解密;

将数据分片解压后的未加密的数据块, 和数据分片中解密的数据块相合并, 得到读取数据;

反馈所述读取数据给终端设备。

本申请实施例还提供一种云系统, 包括: 位于私有云内的至少一个终端设备, 10 网关, 与所述网关连接的加密芯片; 位于公有云内的存储转换服务器和存储设备;

其中, 所述网关, 用于获取待存储数据; 从待存储数据中确定需加密的部分数据, 得到第一目标数据; 获取所述第一目标数据进行加密后的第一密文; 其中, 根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密; 根据所述第一密文生成包含所述第一密文的第二目标数据; 根据所述第二目标数 15 据生成所述第二目标数据对应的数据分片; 将所述第二目标数据对应的所述数据分片传输至公有云中存储;

所述存储转换服务器, 用于根据所述数据分片生成存储数据, 并将所述存储数据更新到存储设备上。

本申请实施例还提供一种混合云的数据存储方法, 应用于加密芯片, 所述方法包括: 20

获取私有云的网关传输的待存储数据中需加密的目标数据;

根据密钥对所述目标数据进行加密, 得到第一密文;

输出所述第一密文至所述网关, 以便所述网关根据所述第一密文确定存储至公有云中的数据。

25 本申请实施例还提供一种加密芯片, 包括至少一个存储器和至少一个处理器, 所述存储器存储有程序, 所述处理器调用所述程序; 所述程序用于:

获取私有云的网关传输的待存储数据中需加密的目标数据;

根据密钥对所述目标数据进行加密, 得到第一密文;

30 输出所述第一密文至所述网关, 以便所述网关根据所述第一密文确定存储至公有云中的数据。

附图说明

35 为了更清楚地说明本申请实施例或现有技术中的技术方案, 下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍, 显而易见地, 下面描述中的附图仅仅是本申请的实施例, 对于本领域普通技术人员来讲, 在不付出创造性劳动的前提下, 还可以根据提供的附图获得其他的附图。

图 1 为本申请实施例提供的混合云的云系统的架构框图;

图 2A 为本申请实施例提供的混合云的数据存储方法的流程图;

图 2B 为本申请实施例提供的混合云的数据存储方法的信令流程图;

40 图 3 为混合云的数据存储方法的另一信令流程图;

图 4 为生成存储数据并更新到存储对象的方法流程图;

图 5 为网关和加密芯片交互实现部分数据加密的示意图；
图 6 为混合云的数据存储方法的再一信令流程图；
图 7 为本申请实施例提供的混合云的数据存储方法的流程图；
图 8 为本申请实施例提供的混合云的数据读取方法的信令流程图；
5 图 9 为本申请实施例提供的混合云的数据存储装置的结构框图；
图 10 为混合云的数据存储装置的另一结构框图；
图 11 为混合云的数据存储装置的再一结构框图；
图 12 为网关的硬件结构框图；
图 13 为本申请实施例提供的混合云的数据读取装置的结构框图。

10 实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

15 图 1 为本申请实施例提供的混合云的云系统的架构框图，通过图 1 所示云系统可实现本申请实施例提供的混合云的数据存储方法，达到提升私有云存储在公有云中的数据的安全性的目的；

参照图 1，该云系统包括：至少一个终端设备 10，网关 20，加密芯片 30，存储转换服务器 40 和存储设备 50；其中，至少一个终端设备 10，网关 20 和加密芯片 30 位于私有云内，存储转换服务器 40 和存储设备 50 位于公有云内；私有云和公有云可通过特定安全协议进行通信，如私有云和公有云可通过 SSL(Secure Sockets Layer 安全套接层)协议进行通信；

如图 1 所示，私有云内的至少一个终端设备 10 可以认为是私有云中具有数据存储和读写需求的终端设备，终端设备 10 的形式可以不限于智能手机、平板电脑、PC(个人计算机)等至少一种用户侧的电子设备；在本申请实施例中，私有云中的该至少一个终端设备 10 可与私有云中的网关 20 通信连接，在终端设备 10 需将数据存储到公有云中时，终端设备 10 可将数据传输给私有云的网关 20，由网关 20 处理后发送到公有云中；

私有云内的网关 20 可以认为是存储网关，作为私有云和公有云间的桥梁，网关 20 连接有加密芯片 30，加密芯片 30 存储有用于进行数据加密的密钥；在一些实施例中，加密芯片 30 可以选用 usb key(usb 钥匙)，usb key 可以内置单片机或智能卡芯片，其有一定的存储空间，可以存储密钥；

网关 20 获取到待存储数据时，可使用本申请实施例提供的混合云的数据存储方法，利用加密芯片 30 所提供的密钥对该待存储数据的全部或部分进行加密(进行加密的操作可以由加密芯片 30 或者网关 20 实现)，从而网关 20 获取到加密后的密文，可根据包含密文的目标待存储数据生成数据分片，并传输到公有云中进行存储；

公有云中的存储转换服务器 40 可获取私有云中的网关所传输的数据分片，可对该数据分片进行协议转换等存储转换处理，使得数据符合存储设备的协议，从而将处理后的数据存储到存储设备 50 中；

存储设备 50 可以认为是一数据存储体系结构，优选使用对象存储。

可见,本申请实施例可在私有云内的网关上连接加密芯片,该加密芯片存储有加密的密钥,利用加密芯片提供的密钥,本申请实施例可对待存储数据的部分或全部进行加密,从而使得存储到公有云中的数据包含以加密芯片提供的密钥所加密的密文,提升存储到公有云中的数据的安全性;而且,加密所使用的密钥由私有云内的网关所连接的加密芯片存储,减小了密钥被管理员获取而导致数据解密泄露的隐患,就算公有云被黑客攻击而导致公有云中的数据泄露,也会因为缺少密钥而降低数据被解密泄露的隐患,进一步提升了私有云存储在公有云中的数据的安全性。

基于图 1 所示的云系统,本申请实施例提供了一种混合云的数据存储方法,应用于私有云的网关。图 2A 为本申请实施例提供的一种混合云的数据存储方法的流程图。如图 2A 所示,该混合云的数据存储方法包括以下步骤:

步骤 201: 获取待存储数据。

步骤 202: 从待存储数据中确定需加密的部分数据,得到第一目标数据。

在一些实例中,确定待存储数据中需加密的部分数据的大小,以及确定需加密的部分数据在待存储数据中相应的位置;根据所述大小和所述位置,从待存储数据中确定需加密的部分数据,并将所述部分数据作为所述第一目标数据。

在一些实例中,确定需加密的部分数据在待存储数据中相应的位置时,确定需加密的部分数据在待存储数据中相应的块内地址偏移。

步骤 203: 获取所述第一目标数据进行加密后的第一密文;其中,根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密。

在一些实施例中,将所述第一目标数据传输至所连接的加密芯片;从所述加密芯片获取所述第一密文,其中,所述加密芯片根据所存储的所述第一密钥,对所述目标数据进行加密以生成所述第一密文。

步骤 204: 根据所述第一密文生成包含所述第一密文的第二目标数据。

在一些实施例中,根据所述块内地址偏移,将所述第一密文覆盖到所述待存储数据中所述第一目标数据的原始位置,得到所述第二目标数据。

步骤 205: 根据所述第二目标数据生成所述第二目标数据对应的数据分片。

步骤 206: 将所述第二目标数据对应的所述数据分片传输至公有云中存储。

在一些实施例中,还可以调取设置表格;当所述设置表格指示由加密芯片进行加密时,触发执行所述将所述第一目标数据传输至所连接的加密芯片的步骤。

在一些实施例中,确定待存储数据中需加密的部分数据的大小包括:确定所述设置表格记录的待存储数据中需加密的部分数据的大小;所述确定需加密的部分数据在待存储数据中相应的位置包括:确定所述设置表格记录的需加密的部分数据在待存储数据中相应的位置。

在一些实施例中,若所述设置表格指示对待存储数据部分加密,触发执行所述从待存储数据中确定需加密的部分数据的步骤。

在一些实施例中,当所述设置表格指示对所述待存储数据进行全部加密,获取所述待存储数据进行加密后的第二密文;其中,根据所述网关所连接的加密芯片提供的第二密钥对所述待存储数据进行加密;根据所述第二密文生成所述第二密文对应的数据分片,并传输至公有云中存储。

在一些实施例中,所述获取待存储数据进行加密后的第二密文包括:判断上一次向所述加密芯片请求的所述第二密钥,是否处于设定的生命周期内;当所述

第二秘钥，处于设定的生命周期内时，获取所述第二秘钥，根据所述第二秘钥对所述待存储数据进行加密，得到第二密文；如果所述第二秘钥，不处于设定的生命周期内，向加密芯片请求第三秘钥，根据请求得到的所述第三秘钥对所述待存储数据进行加密，得到第二密文。

- 5 在一些实施例中，判断所获取的待存储数据的地址空间，是否与设置表格中记录的需加密的待存储数据的地址空间相对应；及根据设置表格中记录的需加密的待存储数据的存储频次，判断所获取的待存储数据是否需要加密；如果判断结果均为是，触发执行所述从待存储数据中确定需加密的部分数据的步骤。

- 10 在一些实例中，上述第一秘钥、上述第二秘钥和上述第三秘钥可以是相同的秘钥，也可以是具有不同秘钥标识的不同的秘钥。

- 本申请实施例可在私有云内的网关上连接加密芯片，该加密芯片存储有加密的秘钥，利用加密芯片提供的秘钥，本发明本申请实施例可对待存储数据的部分或全部进行加密，从而使得存储到公有云中的数据包含以加密芯片提供的秘钥所加密的密文，提升存储到公有云中的数据的安全性；而且，加密所使用的秘钥由
15 私有云内的网关所连接的加密芯片存储，减小了秘钥被管理员获取而导致数据解密泄露的隐患，就算公有云被黑客攻击而导致公有云中的数据泄露，也会因为缺少秘钥而降低数据被解密泄露的隐患，进一步提升了私有云存储在公有云中的数据的安全性。本申请实施例可通过私有云内的网关所连接的加密芯片进行待存储数据的部分加密；基于图 1 所示云系统，图 2B 示出了本申请实施例提供的混合云的数据存储方法的一种可选信令流程图，结合图 1 和图 2B 所示，该信令流程
20 可以包括：

 步骤 S10、私有云内的终端设备向私有云的网关发送数据存储指令，所述数据存储指令携带需存储的数据。

- 25 在一些实施例中，步骤 S10 可由私有云的用户操作终端设备触发，私有云的用户可指定需要存储到公有云的数据，并操作终端设备发送数据存储指令给私有云的网关，指示私有云的网关进行数据至公有云的存储，该数据存储指令可以携带有需存储的数据。

 步骤 S11、私有云的网关获取待存储数据。

- 30 在一些实施例中，本申请实施例可基于数据块进行数据的存储，如果私有云的网关接收到的需存储的数据较大，则可对该需存储的数据进行数据块分块处理，得到多个数据块，从而将各数据块分别作为待存储数据；本申请实施例分块得到的数据块的大小可选为 1（兆），显然，具体数据块的大小可以根据实际情况调整设置；

- 35 而如果私有云的网关接收到的需存储的数据较小，并不足以分块，比如需存储的数据仅为 5k（字节）大小，则本申请实施例可直接将需存储的数据作为待存储数据。

- 在一些实施例中，网关可对外提供虚拟 iscsi（Internet Small Computer System Interface，小型计算机系统接口）块存储设备，即通过 iscsi 接口提供块存储卷，这个存储卷是个线性的地址空间；即对于私有云内的终端设备而言，私有云的网
40 关可以实现一个 iscsi 的 target（iscsi 的存储设备），在私有云的终端设备看来，网关可以是一个块存储设备的接口，可以虚拟多个 volume（卷）供多台终端设备使用；

 在一些实施例中，网关可利用 iscsi 接口提供的块存储卷对需存储的数据进

行数据块分块处理，从而获取到待存储数据；

需要说明的是，网关提供的 iscsi 接口可以与硬盘的块存储接口类似，硬盘的块存储接口对数据的存取是按照扇区号标志的，比如一个 100M(兆)的文件，先通过文件系统管理，最终存储到硬盘上的一组扇区上，这组扇区可能是连续的，也可能是非连续的，具体存储到哪些扇区，是由文件系统决定的；而本申请实施

5 例中，私有云的网关对外提供的虚拟 iscsi 块存储设备，实现的是跟硬盘同层的存储设备，管理的是类似于扇区的数据块；而正常硬盘的一个数据块就是一个扇区，一般是 512 K(字节)，本申请实施例中网关可根据设定将待存储数据分块成更大的数据块进行管理，如 1M 等，具体的数据块的大小可根据实际情况设定。

10 步骤 S12、网关确定所述待存储数据中需加密的部分数据，得到目标数据。
如果需存储的数据分块得到多个数据块，本申请实施例可将各数据块分别作为待存储数据，确定各数据块中需加密的部分数据，得到目标数据；而如果待存储数据较小，可直接将终端设备发送的需存储的数据作为待存储数据，则本申请实施例可确定待存储数据中需加密的部分数据，得到目标数据。

15 在一些实施例中，本申请实施例可由私有云的网关连接的加密芯片进行加密操作，加密芯片可以对待存储数据的部分数据进行加密；

显然，本申请实施例也可对待存储数据的全部进行加密；在一些实施例中，加密芯片具体是對待存储数据的全部或者部分进行加密可以由网关的设置表格记录，该设置表格记录的内容可由用户进行修改调整；如果所述设置表格中记录

20 的是加密芯片加密待存储数据的全部数据，则本申请实施例可对待存储数据的全部进行加密；如果所述设置表格中记录的是加密芯片加密待存储数据的部分数据，则本申请实施例可确定待存储数据中需加密的部分数据，得到目标数据。

步骤 S13、网关将所述目标数据传输至所连接的加密芯片。

25 在一些实施例中，网关与加密芯片可采用 usb 连接，网关可通过 usb 通信协议，将所述目标数据传输至加密芯片。

步骤 S14、加密芯片根据所存储的密钥对所述目标数据进行加密，并向所述网关返回加密后的第一密文。

加密芯片获取到网关所传输的目标数据后，可根据加密芯片内存储的密钥对所述目标数据进行加密，得到加密后的第一密文；加密芯片可将加密后的第一密文反馈给网关；第一密文可以认为是待存储数据中的部分数据加密后的密文；

30 密钥可以认为是一组特定的秘密数据，在加密时，密钥控制加密算法按照指定的方式将明文变换为相应的密文，并将一组信源标识信息变换不可伪造的签名；在解密时，它控制解密算法按照指定的方式将密文变换为相应的明文，并将签名信息变换成不可否认的信源证据；

35 在一些实施例中，本申请实施例所使用的加密算法可以根据实际情况设定。

步骤 S15、网关根据所述第一密文生成包含所述第一密文的目标待存储数据。

40 在一些实施例中，如果加密芯片是對待存储数据的部分数据进行加密，则加密后的第一密文是待存储数据中部分的数据进行加密后结果，本申请实施例可将第一密文覆盖到待存储数据中目标数据的原始位置，从而生成包含所述第一密文的目标待存储数据。

步骤 S16、网关根据所述目标待存储数据生成数据分片。

在一些实施例中，本申请实施例可确定目标待存储数据的元数据，将该元数据与目标待存储数据结合生成数据分片；在一些实施例中，本申请实施例可将目

标待存储数据进行压缩后,与元数据结合生成数据分片;

- 5 在一些实施例中,元数据的内容可以包括如下至少一项:待存储数据是否为完整数据块的指示信息,块内地址偏移,待存储数据的数据长度,待存储数据部分加密还是全部加密的指示信息,密文的内部偏移,密文的数据长度,由加密芯片还是网关加密的加密方式指示信息,当前使用密钥的密钥 id 或种子 id,加密算法的指示信息,压缩算法的指示信息等。

其中,密钥 id (身份标识号)与加密芯片当前所使用的密钥相对应,加密芯片所存储的一密钥可对应一密钥 id;种子 id 与生成密钥所使用的种子相对应,一种子对应一种子 id。

- 10 步骤 S17、网关将所述数据分片传输至公有云。

在一些实施例中,网关将所述数据分片传输至公有云中存储,公有云中的存储转换服务器可接收所述数据分片。

步骤 S18、公有云的存储转换服务器根据所述数据分片生成存储数据,并将所述存储数据更新到对象存储上。

- 15 在一些实施例中,视待存储数据是否为完整数据块,存储转换服务器根据数据分片生成存储数据的处理过程可能不同;待存储数据是否为完整数据块,可以由数据分片中的元数据记录的待存储数据是否为完整数据块的指示信息确定;

- 20 如果待存储数据为完整的数据块,则存储转换服务器可直接将数据分片与特定存储数据内容相结合,生成存储数据;从而可将存储数据中的数据分片的目标待存储数据,覆盖到对象存储中以前存储的相应数据上,同时在对象存储中记录相应的元数据与特定存储数据内容;

- 25 在一些实施例中,如果待存储数据不为完整的数据块,比如待存储数据仅是 5k 的数据,并不满足 1M 大小完整需求的数据块,则存储转换服务器可从存储设备中取回待存储数据相应的至少一个原数据分片;对取回的各原数据分片进行逐片解压,得到至少一个原数据块,合并目标待存储数据与所述至少一个原数据块,得到至少一个需存储的数据块,将至少一个需存储的数据块进行压缩,压缩后的数据与元数据结合形成数据分片,所形成的数据分片和特定存储数据内容相结合,生成存储数据,从而将存储数据更新到对象存储中。

- 30 在一些实施例中,存储转换服务器还可在数据分片的协议与存储设备的协议不一致时,将数据分片的协议转换为与存储设备的协议相一致。

存储设备可在记录存储数据时,按照数据块的地址空间分配不同的块,存储数据的一个数据块对应一个文件,使用标识值 (bno) 来标识数据块的块号;bno 通过地址和块大小计算,比如 1M 大小为 1 块,第 0-1M 字节内 bno 是 0,1-2M 的 bno 是 1,其他类似;地址 mod 块大小可以认为是 bno。

- 35 在一些实施例中,特定存储数据内容可以包括如下至少一项:数据属性(数据块的版本号),数据头-定长(协议版本、数据块版本号、分片数量);

相应的,存储数据的结构可以如下:

数据属性,包括:数据块的版本号;

数据头-定长,包括:协议版本、数据块版本号、分片数量;

- 40 数据分片-定长(即元数据),包括:待存储数据是否为完整数据块的指示信息,块内地址偏移,待存储数据的数据长度,部分加密还是全部加密的指示信息,密文的内部偏移,密文的数据长度,由加密芯片还是网关加密的加密方式指示信息,当前使用密钥的密钥 id 或种子 id,加密算法,压缩算法等;

数据分片-变长, 包括: 具体的数据块。

可见, 基于图 2 所示信令流程, 在将私有云中的数据存储在公有云时, 本申请实施例可利用私有云的网关所连接的加密芯片提供的密钥, 对待存储数据的部分进行加密, 从而将包含加密后的第一密文的目标待存储数据进行至公有云的存储; 由于目标待存储数据包含以加密芯片提供的密钥所加密的第一密文, 提升了存储到公有云中的数据的安全性, 并且加密所使用的密钥由加密芯片存储, 密钥泄露的风险极低, 可降低由于云管理员泄露数据、公有云被黑客攻击等情况下的数据泄露风险, 提升了私有云存储在公有云中的数据的安全性。

10 在一些实施例中, 在图 2 所示信令流程中, 加密芯片可对待存储数据的部分进行加密, 但也不排除加密芯片对待存储数据的全部进行加密的情况; 作为优选, 由于加密芯片的加密性能可能较差, 并无法对待存储数据的全部进行加密, 因此本申请实施例可优选使用加密芯片对待存储数据的部分进行加密; 显然, 这仅是由加密芯片进行加密操作的一种优选方案, 本申请实施例并不排除加密芯片在具有足够的加密性能时, 由加密芯片对待存储数据的全部进行加密的情况。

15 在一些实施例中, 图 3 示出了本申请实施例提供的混合云的数据存储方法的另一种可选信令流程, 结合图 1 和图 3 所示, 该信令流程可以包括:

步骤 S20、私有云内的终端设备向私有云的网关发送数据存储指令。

步骤 S21、私有云的网关获取待存储数据。

20 步骤 S22、网关确定待存储数据中需加密的部分数据的大小, 以及确定需加密的部分数据在待存储数据中相应的位置; 根据所述大小和所述位置, 从待存储数据中确定需加密的部分数据, 得到目标数据。

25 在一些实施例中, 本申请实施例可确定待存储数据中需加密的部分数据的大小, 以及需加密的部分数据在待存储数据中相应的位置 (如待存储数据为数据块时, 需加密的部分数据在待存储数据中相应的块内地址偏移), 从而根据所设定的需加密的部分数据的大小以及在待存储数据中相应的位置, 从待存储数据中确定需加密的部分数据, 得到目标数据;

30 在一些实施例中, 需加密的部分数据的大小, 以及需加密的部分数据在待存储数据中相应的位置可记录在设置表格中, 并由用户进行修改调整; 例如, 设置表格可记录需加密的部分数据的大小, 以及需加密的部分数据在待存储数据中相应的块内地址偏移; 相应的, 本申请实施例可确定所述设置表格记录的待存储数据中需加密的部分数据的大小, 确定所述设置表格记录的需加密的部分数据在待存储数据中相应的位置。

35 在一些实施例中, 需加密的目标数据相应的块内地址偏移可以认为是, 进行加密的目标数据 (部分数据) 在待存储数据中的起始地址, 比如一个待存储数据的大小是 1M, 对该 1M 的待存储数据中 2K 的目标数据进行加密, 则这个 2K 的目标数据在待存储数据的起始地址则认为是, 这个 2K 的目标数据加密后的第一密文相应的块内地址偏移。

40 例如, 在待存储数据为通过数据块分块处理得到的数据块时, 在设定需加密的部分数据的大小为 2k (数值仅是可选示例), 及需加密的部分数据相应的块内地址偏移后, 网关可从待存储数据中该块内地址偏移开始, 选取 2k 的数据作为需加密的部分数据, 得到目标数据;

在一些实施例中, 本申请实施例也可随机的确定待存储数据中需加密的部分

数据的大小，以及需加密的部分数据在待存储数据中相应的位置。

步骤 S23、网关将所述目标数据传输至所连接的加密芯片。

步骤 S24、加密芯片根据所存储的秘钥对所述目标数据进行加密，并向所述网关返回加密后的第一密文。

- 5 步骤 S25、网关从待存储数据中目标数据的起始位置开始，覆盖所述第一密文，得到包含所述第一密文的目标待存储数据。

10 在一些实施例中，网关获取到第一密文后，可确定第一密文相对应的需加密的部分数据在待存储数据中相应的块内地址偏移，从而根据该块内地址偏移，将第一密文覆盖到待存储数据中目标数据的原始位置，得到包含所述第一密文的目标待存储数据；即按照该块内地址偏移，从待存储数据中目标数据的起始位置开始，覆盖所述第一密文，得到包含所述第一密文的目标待存储数据。

步骤 S26、网关根据所述目标待存储数据生成数据分片。

在一些实施例中，可结合目标待存储数据的元数据与目标待存储数据，生成数据分片；元数据的内容可参照上文描述。

- 15 步骤 S27、网关将所述数据分片传输至公有云。

步骤 S28、公有云的存储转换服务器根据所述数据分片生成存储数据，并将所述存储数据更新到对象存储上。

20 在一些实施例中，步骤 S28 的说明可与图 2 所示步骤 S18 类似，需要进一步说明的是，如果待存储数据不为完整的数据块，则将解压原数据分片得到的至少一个原数据块与目标待存储数据合并，得到至少一个需存储的数据块的过程可以为：

25 如果对取回的各原数据分片进行逐片解压后的原数据块，与目标待存储数据不存在加密数据交叉的情况，则可将原数据块与目标待存储数据合并为一个完整数据块；而如果原数据块，与目标待存储数据存在加密数据交叉的情况，则可将与目标待存储数据存在加密数据交叉的原数据块相独立，将与目标待存储数据不存在加密数据交叉的原数据块，和目标待存储数据进行合并，从而集合相独立的原数据块，和合并后的数据块，得到至少一个需存储的数据块；

在一些实施例中，步骤 S28 的执行流程可以如图 4 所示，包括：

- 30 步骤 S100、判断待存储数据是否为完整的数据块，若是，执行步骤 S110，若否，执行步骤 S130。

在一些实施例中，可通过数据分片中的元数据记录的待存储数据是否为完整数据块的指示信息确定，待存储数据是否为完整的数据块。

步骤 S110、将数据分片与特定存储数据内容相结合，生成存储数据。

在一些实施例中，数据分片可以包括：目标待存储数据与相应的元数据。

- 35 步骤 S120、将存储数据中的目标待存储数据覆盖到对象存储中以前存储的相应数据上，同时在对象存储中记录存储数据相应的元数据与特定存储数据内容。

步骤 S130、从对象存储中取回待存储数据的至少一个原数据分片。

40 比如待存储数据为 5K，对象存储以 1M 的数据块进行数据存储，则可从对象存储中取回该 5K 的待存储数据所对应的，在对象存储中以 1M 的数据块进行存储的原数据分片。

步骤 S140、对取回的各原数据分片进行逐片解压，得到至少一个原数据块。

步骤 S150、判断原数据块与目标待存储数据是否存在加密数据交叉，若是，执行步骤 S160，若否，执行步骤 S170。

在一些实施例中，本申请实施例可通过目标待存储数据和原数据块中加密数据的地址空间及加密数据的长度，判断原数据块与目标待存储数据是否存在加密数据交叉，比如目标待存储数据中加密数据的地址空间为 4-7，原数据块中加密数据的地址空间为 16-19，则不存在加密数据交叉，而如果目标待存储数据中加密数据的地址空间为 4-7，原数据块中加密数据的地址空间为 6-9，则存在加密数据交叉。

步骤 S160、将与目标待存储数据存在加密数据交叉的原数据块相独立，并将与目标待存储数据不存在加密数据交叉的原数据块，和目标待存储数据进行合并，集合相独立的原数据块，和合并后的数据块，得到需存储的数据块。

比如目标待存储数据为包含 2K 的密文的 5K 数据，则在确定原数据块后，可将原数据块中存在加密数据，且加密数据的地址与该 2K 密文的地址交叉的原数据块进行独立，不与目标待存储数据进行合并；而对于原数据块中存在加密数据，但不与该 2K 密文的地址交叉的原数据块，或者原数据块中不存在加密的原数据块，则可目标待存储数据进行合并，得到合并后的数据块；然后可将独立的存在加密数据交叉的原数据块，和合并后的数据块集合起来。

步骤 S170、将原数据块与目标待存储数据合并，得到需存储的数据块。

步骤 S180、需存储的数据块进行压缩，压缩后的数据与元数据结合形成数据分片，所形成的数据分片和特定存储数据内容相结合，生成存储数据，将所述存储数据更新到对象存储上。

相应的，从连接私有云的网关的角度看，网关可获取网关传输的待存储数据中需加密的目标数据，根据密钥对所述目标数据进行加密，得到第一密文；输出所述第一密文至所述网关，以便所述网关根据所述第一密文确定存储至公有云中的数据（可参照网关获取第一密文后的后续处理）。

从私有云内来看，通过加密芯片进行部分数据加密时，加密芯片与网关的交互过程可以如图 5 所示，网关可根据设定的待存储数据中需加密的部分数据的大小，以及需加密的部分数据在待存储数据中相应的位置，确定待存储数据中需加密的部分数据，得到目标数据；将该目标数据传输至加密芯片；加密芯片根据所存储的密钥对目标数据进行加密，并反馈第一密文给网关；网关可按照所述块内地址偏移，从待存储数据中目标数据的原始位置开始覆盖密文，从而得到包含第一密文的目标待存储数据，从而实现对待存储数据中的部分数据进行加密的效果。

在一些实施例中，本申请实施例也可在私有云内的网关上进行加密操作，网关向加密芯片获取一次密钥后，一次获取的密钥可以维持设定的生命周期，网关可利用当前处于设定的生命周期内的密钥进行加密操作；网关也可在每次进行数据的存储时，从加密芯片获取一次密钥进行加密操作，从而利用加密芯片所提供的密钥进行待存储数据中目标数据的加密操作；

在一些实施例中，图 6 示出了本申请实施例提供的混合云的数据存储方法的再一种可选信令流程，结合图 1 和图 6 所示，该信令流程可以包括：

步骤 S30、私有云内的终端设备向私有云的网关发送数据存储指令。

步骤 S31、私有云的网关获取待存储数据。

步骤 S32、网关根据加密芯片所提供的密钥对所述待存储数据进行加密，得到加密后的第二密文。

在一些实施例中，如果所述设置表格指示对待存储数据全部加密，则可将所述待存储数据进行加密，得到第二密文；而如果所述设置表格指示对待存储数据

的部分进行加密,则可按照前述方法内容,确定待存储数据中需加密的部分数据,得到目标数据,由网关或加密芯片对该目标数据进行加密,得到第一密文;

5 在一些实施例中,网关可向所连接的加密芯片请求密钥,从而获取到加密芯片所提供的密钥,进而以该密钥对目标数据进行加密;这种方式是网关在每次进行加密操作时,均向加密芯片请求密钥;

10 在一些实施例中,另一种方式可以是网关向加密芯片请求一次密钥后,所请求得到的密钥可以维持设定的生命周期,如果上一次向加密芯片请求的密钥仍处于设定的生命周期内,则网关可根据上一次向加密芯片请求的密钥对所述待存储数据进行加密;在一些实施例中,上一次向加密芯片请求的密钥可以在网关中进行存储,并维持设定的生命周期有效,当超过设定的生命周期后,网关可再次向加密芯片请求密钥,根据再次请求得到的密钥对所述待存储数据进行加密,得到第二密文;

15 在一些实施例中,一次获取的密钥所维持的设定的生命周期可以是:一次获取的密钥设定的有效时间,或者,一次获取的密钥可以支持网关n次的数据读写;n为设定值,可以根据实际情况设定。

在一些实施例中,网关每次从加密芯片获取的密钥可以是一致的;显然,不排除加密芯片通过动态方式生成动态变化的密钥的情况,但该密钥可通过密钥id相对应。

20 步骤S33、网关根据所述第二密文生成数据分片。

步骤S34、网关将所述数据分片传输至公有云。

步骤S35、公有云的存储转换服务器根据所述数据分片生成存储数据,并将所述存储数据更新到对象存储上。

25 作为优选的,网关可以对待存储数据的全部进行加密。显然,也可由加密芯片对待存储数据的全部进行加密。

30 在一些实施例中,上文描述了由加密芯片加密待存储数据的部分或全部,由网关加密待存储数据的部分或全部的方案,这些方案可以是并列的;基于利用网关连接的加密芯片提供的密钥对存储到公有云的数据进行加密的情况下,这些方案可以择一应用;

显然,这些方案中可以优选使用由加密芯片加密待存储数据的部分,和由网关加密待存储数据的全部的方案;

35 在一些实施例中,在优选方案中,选择加密芯片加密待存储数据的部分,还是由网关加密待存储数据的全部,可以由设置表格进行记录调整。

40 在一些实施例中,在本申请实施例中,设置表格可以记录如下至少一项:

待存储数据部分加密还是全部加密的指示信息;

由加密芯片还是网关加密的加密方式指示信息;

部分加密情况下需加密的部分数据的大小,以及需加密的部分数据在待存储数据中相应的块内地址偏移;

45 加密芯片加密情况下的密钥id,加密算法的指示信息;进一步,加密芯片的管理员可以在加密芯片上设置密钥id和对应的密钥;

网关加密情况下的生成密钥的种子id,加密算法的指示信息;进一步,加密芯片的管理员可以在加密芯片上设置种子id和对应的种子。

50 在一些实施例中,设置表格还可以记录:压缩算法的指示信息。

在一些实施例中，在结合使用由加密芯片加密待存储数据的部分，和由网关加密待存储数据的全部的情况下，图 7 示出了本申请实施例提供的混合云的数据存储方法的流程，该方法可应用于私有云的网关，参照图 7，该方法可以包括：
步骤 S200、获取待存储数据。

5 在一些实施例中，设置表格中还可以记录需进行加密的待存储数据的地址空间（待存储数据的地址空间可以由网关的 iscsi 接口提供块存储卷确定，该存储卷对应一个线性的地址空间，所划分的各数据块（待存储数据的一种形式）可对应有一地址空间），如果所获取的待存储数据的地址空间，与设置表格中记录的需进行加密的待存储数据的地址空间相对应，则可执行图 7 后续流程；否则，则
10 可将该待存储数据以明文方式存储；

在一些实施例中，设置表格中还可记录需进行加密的待存储数据的存储频次，比如每设定次数存储仅进行一次加密，从而可根据设置表格中记录的需进行加密的待存储数据的存储频次，判断所获取的待存储数据是否需要加密，若是，则可执行图 7 后续流程；否则，则可将该待存储数据以明文方式存储；

15 进一步，可结合设置表格中记录的需进行加密的待存储数据的地址空间，和需进行加密的待存储数据的存储频次，来判断是否需要基于所获取的待存储数据执行图 7 后续流程；如果所获取的待存储数据的地址空间，与设置表格中记录的需进行加密的待存储数据的地址空间相对应，且根据设置表格中记录的需进行加密的待存储数据的存储频次，确定所获取的待存储数据需要加密，则可确定执行
20 图 7 后续流程，否则，则可将该待存储数据以明文方式存储。

步骤 S210、根据设置表格中记录的加密方式指示信息，判断是由加密芯片还是由网关进行加密，若由加密芯片进行加密，执行步骤 S220，若由网关进行加密，执行步骤 S260。

25 步骤 S220、根据设置表格中记录的设定的需加密的部分数据的大小以及在待存储数据中相应的块内地址偏移，确定所述待存储数据中需加密的部分数据，得到目标数据。

步骤 S230、将所述目标数据传输给所连接的加密芯片，以便获取到所述加密芯片根据所存储的密钥对所述目标数据进行加密后的第一密文。

30 步骤 S240、按照所述块内地址偏移，从待存储数据中目标数据的起始位置开始覆盖所述第一密文，得到包含所述第一密文的目标待存储数据。

步骤 S250、根据目标待存储数据生成数据分片，并将所述数据分片传输至公有云。

步骤 S260、根据加密芯片所提供的密钥对待存储数据进行加密，得到第二密文。

35 在一些实施例中，在本申请实施例中由加密芯片进行待存储数据的部分加密，由网关进行待存储数据的全部加密。

步骤 S270、根据所述第二密文生成数据分片，并将所述数据分片传输至公有云。

在一些实施例中，第二密文可结合元数据生成数据分片。

40 在一些实施例中，进一步，设置表格中还可记录网关从加密芯片获取密钥的读写间隔次数，如每 n 次读写，网关从加密芯片中获取一次密钥。

本申请实施例可利用加密芯片，根据密钥对待存储数据的部分进行加密，利用网关，根据加密芯片提供的密钥对待存储数据的全部进行加密。从而对待存储

数据的部分或全部进行加密，将包含加密后的密文的数据进行至公有云的存储。

- 由于目标待存储数据包含以加密芯片提供的秘钥所加密的密文，提升了存储到公有云中的数据的安全性；并且加密所使用的秘钥由加密芯片存储，秘钥泄露的风险极低，且加密芯片与网关断开后，基本没有任何途径可以获取到秘钥，降低了由于云管理员泄露数据、公有云被黑客攻击等情况下的数据泄露风险，进一步提升了私有云存储在公有云中的数据的安全性。

- 本申请实施例提供的混合云的数据读取方法的信令流程可以如图 8 所示，该数据读取方法可基于上文描述的数据存储方法实现，参照图 8，该信令流程可以包括：

步骤 S40、私有云内的终端设备向私有云的网关发送数据读取指令。

步骤 S41、网关转发所述数据读取指令至公有云。

- 步骤 S42、公有云的存储转换服务器根据所述数据读取指令，获取存储设备中相应存储的存储数据；所述存储数据包括至少一个数据分片，所述至少一个数据分片包括所述数据读取指令相应读取的数据块，和该数据块相应的元数据。

在一些实施例中，在进行数据读取时，存储设备是以数据块的形式进行数据读取。

- 在一些实施例中，存储设备（如对象存储）中存储的数据块是以标识值（bno）进行表示的，本申请实施例中，数据读取指令中可以携带需读取的数据块的标识值（bno）的指示信息；从而存储转换服务器可根据标识值（bno）的指示信息，从存储设备中获取相应的值（数据块），进而可将包含所获取的数据块和该数据块相应的元数据的数据分片的存储数据，从存储设备中获取出来。

步骤 S43、存储转换服务器发送所述存储数据给私有云的网关。

从而私有云的网关可获取到公有云中的存储数据。

- 步骤 S44、私有云的网关对所述存储数据中的各数据分片进行逐片解压，如果解压过程中，确定数据分片中存在加密的数据块，根据该数据块的元数据选取解密算法，及确定网关连接的加密芯片提供的秘钥。

在一些实施例中，数据分片中存在加密的数据块，可能是该数据块部分或全部被加密，可以由该数据块的元数据进行指示；

- 在一些实施例中，针对数据块的部分解密的过程，与数据块的部分加密的过程可以是逆过程；如果一数据分片在解压过程中，确定该数据分片的数据块存在部分数据被加密，则可根据该数据分片的元数据记录的加密算法选取解密算法，及根据该元数据记录的秘钥 id，获取网关连接的加密芯片提供的相应秘钥；从而可根据所选取的解密算法和获取的秘钥，对该数据分片的数据块中的部分加密的目标数据进行解密，解密后的目标数据可根据相应的块内地址偏移，覆盖到数据块中目标数据的原始位置，获得到该数据分片相应的解密的数据块；

而针对一数据分片的数据块被全部加密的情况，则可根据该数据分片的元数据所确定的解密算法和秘钥，对该数据分片的数据块整体进行解密，获得到该数据分片相应的解密的数据块。

- 步骤 S45、网关根据所述解密算法和秘钥，对数据分片中存在加密的数据块进行解密。

在一些实施例中，解密操作可以由网关实现。

步骤 S46、网关将数据分片解压后的未加密的数据块，和数据分片中解密的

数据块相合并，得到读取数据，并反馈所述读取数据给终端设备。

需要说明的，针对待存储数据的部分或全部进行加密的情况下，数据读取和存储可以认为是逆过程，可以相互参照。

- 5 下面对本申请实施例提供的混合云的数据存储装置进行介绍，下文描述的混合云的数据存储装置可以认为是，私有云的网关为实现本申请实施例提供的混合云的数据存储方法所需设置的程序模块；下文描述的混合云的数据存储装置内容，可与上文描述的混合云的数据存储方法内容相互对应参照。

10 图 9 为本申请实施例提供的混合云的数据存储装置的结构框图，该混合云的数据存储装置可应用于私有云的网关，参照图 9，该混合云的数据存储装置可以包括：

待存储数据获取模块 100，用于获取待存储数据；

目标数据确定模块 110，用于从待存储数据中确定需加密的部分数据，得到目标数据；

- 15 密文获取模块 120，用于获取所述目标数据进行加密后的第一密文；其中，所述目标数据根据所述网关所连接的加密芯片提供的密钥进行加密；

目标待存储数据确定模块 130，用于根据所述第一密文生成包含所述第一密文的目标待存储数据；

数据分片确定模块 140，用于根据所述目标待存储数据生成数据分片；

- 20 传输模块 150，用于将所述数据分片传输至公有云中存储。

在一些实施例中，目标数据确定模块 110，用于从待存储数据中确定需加密的部分数据，得到目标数据，具体包括：

确定待存储数据中需加密的部分数据的大小，以及确定需加密的部分数据在待存储数据中相应的位置；

- 25 根据所述大小和所述位置，从待存储数据中确定需加密的部分数据。

在一些实施例中，目标数据确定模块 110 可确定设置表格记录的待存储数据中需加密的部分数据的大小，及确定设置表格记录的需加密的部分数据在待存储数据中相应的位置。

- 30 在一些实施例中，目标数据确定模块 110，用于确定需加密的部分数据在待存储数据中相应的位置，具体包括：

确定需加密的部分数据在待存储数据中相应的块内地址偏移。

在一些实施例中，目标待存储数据确定模块 130，用于根据所述第一密文生成包含所述第一密文的目标待存储数据，具体包括：

- 35 根据所述块内地址偏移，将第一密文覆盖到待存储数据中目标数据的原始位置，得到所述目标待存储数据。

在一些实施例中，密文获取模块 120，用于获取所述目标数据进行加密后的第一密文，具体包括：

将所述目标数据传输至所连接的加密芯片；

- 40 获取所述加密芯片根据所存储的密钥，对所述目标数据进行加密后的第一密文。

在一些实施例中，图 10 示出了本申请实施例提供的混合云的数据存储装置的另一结构框图，结合图 9 和图 10 所示，该装置还可以包括：

表格调取模块 160，用于调取设置表格；

加密执行第一确定模块 170, 用于如果所述设置表格指示由加密芯片进行加密, 触发密文获取模块 120 执行所述将所述目标数据传输至所连接的加密芯片的步骤。

在一些实施例中, 所述设置表格还记录有如下至少一项内容:

- 5 待存储数据部分加密还是全部加密的指示信息;
待存储数据中需加密的部分数据的大小, 以及需加密的部分数据在待存储数据中相应的块内地址偏移;
加密芯片加密所使用的密钥 id, 加密算法的指示信息;
网关使用加密芯片提供的密钥进行加密时, 生成密钥的种子 id, 加密算法的指示信息;
10 压缩算法的指示信息;
网关从加密芯片获取密钥的读写间隔次数。

在一些实施例中, 所述数据存储装置还可用于:

- 若所述设置表格指示对待存储数据部分加密, 触发目标数据确定模块 110 执行所述从待存储数据中确定需加密的部分数据的步骤。

在一些实施例中, 所述数据存储装置还可用于:

- 如果所述设置表格指示对待存储数据全部加密, 获取待存储数据进行加密后的第二密文, 其中, 所述待存储数据根据所述网关所连接的加密芯片提供的密钥进行加密; 根据第二密文生成数据分片, 并传输至公有云中存储。

- 20 在一些实施例中, 所述数据存储装置用于获取待存储数据进行加密后的第二密文, 具体包括:

获取加密芯片提供的密钥;

根据所述密钥对所述待存储数据进行加密, 得到第二密文。

- 25 在一些实施例中, 所述数据存储装置用于获取加密芯片提供的密钥, 具体包括:

判断上一次向加密芯片请求的密钥, 是否处于设定的生命周期内;

如果上一次向加密芯片请求的密钥, 处于设定的生命周期内, 获取上一次向加密芯片请求的密钥;

- 30 如果上一次向加密芯片请求的密钥, 不处于设定的生命周期内, 向加密芯片请求密钥。

在一些实施例中, 数据分片确定模块 140, 用于根据所述目标待存储数据生成数据分片, 具体包括:

确定目标待存储数据的元数据, 将该元数据与目标待存储数据结合生成数据分片。

- 35 在一些实施例中, 元数据可以包括如下至少一项内容:

待存储数据是否为完整数据块的指示信息, 块内地址偏移, 待存储数据的数据长度, 待存储数据部分加密还是全部加密的指示信息, 密文的内部偏移, 密文的数据长度, 由加密芯片还是网关加密的加密方式指示信息, 当前使用密钥的密钥 id 或种子 id, 加密算法的指示信息, 压缩算法的指示信息。

- 40 在一些实施例中, 所述设置表格中还记录有需进行加密的待存储数据的地址空间, 需进行加密的待存储数据的存储频次; 结合图 10 和图 11 所示, 图 11 所示的本申请实施例提供的混合云的数据存储装置还可以包括:

加密触发判断模块 180, 用于判断所获取的待存储数据的地址空间, 是否与

设置表格中记录的需进行加密的待存储数据的地址空间相对应；及，根据设置表格中记录的需进行加密的待存储数据的存储频次，判断所获取的待存储数据是否需要加密；

- 5 如果所获取的待存储数据的地址空间，与设置表格中记录的需进行加密的待存储数据的地址空间相对应，且根据设置表格中记录的需进行加密的待存储数据的存储频次，确定所获取的待存储数据需要加密，则触发目标数据确定模块 110 执行所述从待存储数据中确定需加密的部分数据的步骤。

本申请实施例还提供一种私有云的网关，该网关的硬件结构框图可以如图 12 所示，包括：至少一个处理器 1，至少一个通信接口 2，至少一个存储器 3 和
10 至少一个通信总线 4；

在本申请实施例中，处理器 1、通信接口 2、存储器 3、通信总线 4 的数量为至少一个，且处理器 1、通信接口 2、存储器 3 通过通信总线 4 完成相互间的通信；

15 在一些实施例中，通信接口 2 可以为通信模块的接口，如 GSM 模块的接口；

处理器 1 可能是一个中央处理器 CPU，或者是特定集成电路 ASIC (Application Specific Integrated Circuit)，或者是被配置成实施本申请实施例的一个或多个集成电路。

20 存储器 3 可能包含高速 RAM 存储器，也可能还包括非易失性存储器 (non-volatile memory)，例如至少一个磁盘存储器。

其中，存储器 3 存储有程序，处理器 1 调用存储器 3 所存储的程序，该程序具体用于：

- 获取待存储数据；
从待存储数据中确定需加密的部分数据，得到目标数据；
25 获取所述目标数据进行加密后的第一密文；其中，所述目标数据根据所述网关所连接的加密芯片提供的密钥进行加密；
根据所述第一密文生成包含所述第一密文的目标待存储数据；
根据所述目标待存储数据生成数据分片；
将所述数据分片传输至公有云中存储。

30 本申请实施例还可提供一种存储介质，存储介质的形式可如存储器等，该存储介质可应用于私有云的网关，该存储介质中可记录程序，该程序可用于：

- 获取待存储数据；
从待存储数据中确定需加密的部分数据，得到目标数据；
获取所述目标数据进行加密后的第一密文；其中，所述目标数据根据所述网
35 关所连接的加密芯片提供的密钥进行加密；
根据所述第一密文生成包含所述第一密文的目标待存储数据；
根据所述目标待存储数据生成数据分片；
将所述数据分片传输至公有云中存储。

40 在一些实施例中，程序的功能细化和扩展功能可参照上文相应部分描述。

在一些实施例中，本申请实施例还提供一种加密芯片，该加密芯片可以包括：至少一个存储器和至少一个处理器，所述存储器存储有程序，所述处理器调用所述程序，所述程序用于：

获取私有云的网关传输的待存储数据中需加密的目标数据；

根据秘钥对所述目标数据进行加密，得到第一密文；

输出所述第一密文至所述网关，以便所述网关根据所述第一密文确定存储至公有云中的数据。

- 5 本申请实施例还提供一种混合云的数据读取装置，该混合云的数据读取装置可以认为是私有云的网关，为实现本申请实施例提供的混合云的数据读取方法所需设置的程序模块；下文描述的混合云的数据读取装置，可与上文描述的混合云的数据读取方法相互对应参照。

- 10 图 13 为本申请实施例提供的混合云的数据读取装置的结构框图，该装置可应用于私有云的网关，参照图 13，该混合云的数据读取装置可以包括：

存储数据获取模块 200，用于获取公有云中的存储数据；所述存储数据包括至少一个数据分片，所述至少一个数据分片包括需读取的数据块，和该数据块相应的元数据；

- 15 解压模块 210，用于对所述存储数据中的各数据分片进行逐片解压，如果解压过程中，确定数据分片中存在加密的数据块，根据该数据块的元数据选取解密算法，及确定网关连接的加密芯片提供的秘钥；

解密模块 220，用于根据所述解密算法和秘钥，对数据分片中存在加密的数据块进行解密；

- 20 读取数据得到模块 230，用于将数据分片解压后的未加密的数据块，和数据分片中解密的数据块相合并，得到读取数据；

数据反馈模块 240，用于反馈所述读取数据给终端设备。

在一些实施例中，解密模块 220，用于根据所述解密算法和秘钥，对数据分片中存在加密的数据块进行解密，具体包括：

- 25 如果数据分片的数据块存在部分数据被加密，根据所选取的解密算法和获取的秘钥，对该数据分片的数据块中的部分加密的目标数据进行解密，解密后的目标数据根据相应的块内地址偏移，覆盖到数据块中目标数据的原始位置，获得相应解密的数据块。

- 30 在一些实施例中，上文描述的混合云的数据读取装置可以通过程序模块形式，装载在私有云的网关内；相应的，网关的结构可以如图 12 所示，包括：至少一个处理器 1，至少一个通信接口 2，至少一个存储器 3 和至少一个通信总线 4；

其中，存储器存储有程序，处理器调用所述程序；所述程序用于：

获取公有云中的存储数据；所述存储数据包括至少一个数据分片，所述至少一个数据分片包括需读取的数据块，和该数据块相应的元数据；

- 35 对所述存储数据中的各数据分片进行逐片解压，如果解压过程中，确定数据分片中存在加密的数据块，根据该数据块的元数据选取解密算法，及确定网关连接的加密芯片提供的秘钥；

根据所述解密算法和秘钥，对数据分片中存在加密的数据块进行解密；

将数据分片解压后的未加密的数据块，和数据分片中解密的数据块相合并，得到读取数据；

- 40 反馈所述读取数据给终端设备。

在一些实施例中，本申请实施例还提供一种云系统，该云系统的结构可以如图 1 所示，包括：位于私有云内的至少一个终端设备，网关，与所述网关连接的

加密芯片；位于公有云内的存储转换服务器和存储设备；

- 其中，所述网关，用于获取待存储数据；从待存储数据中确定需加密的部分数据，得到目标数据；获取所述目标数据进行加密后的第一密文；其中，所述目标数据根据所述网关所连接的加密芯片提供的密钥进行加密；根据所述第一密文生成包含所述第一密文的目标待存储数据；根据所述目标待存储数据生成数据分片；将所述数据分片传输至公有云中存储；

所述存储转换服务器，用于根据所述数据分片生成存储数据，并将所述存储数据更新到对象存储上。

- 在一些实施例中，存储转换服务器，用于根据所述数据分片生成存储数据，具体包括：

如果待存储数据为完整的数据块，则将数据分片与特定存储数据内容相结合，生成存储数据；

- 如果待存储数据不为完整的数据块，则从存储设备中取回待存储数据相应的至少一个原数据分片；对取回的各原数据分片进行逐片解压，得到至少一个原数据块，合并目标待存储数据与所述至少一个原数据块，得到至少一个需存储的数据块；将至少一个需存储的数据块进行压缩，压缩后的数据与元数据结合形成数据分片，所形成的数据分片和特定存储数据内容相结合，生成存储数据。

在一些实施例中，存储转换服务器，用于合并目标待存储数据与所述至少一个原数据块，得到至少一个需存储的数据块，具体包括：

- 判断原数据块与目标待存储数据是否存在加密数据交叉；

若是，将与目标待存储数据存在加密数据交叉的原数据块相独立，并将与目标待存储数据不存在加密数据交叉的原数据块，和目标待存储数据进行合并，集合相独立的原数据块，和合并后的数据块，得到需存储的数据块；

若否，将原数据块与目标待存储数据合并，得到需存储的数据块。

- 在一些实施例中，所述网关，还用于获取公有云中的存储数据；所述存储数据包括至少一个数据分片，所述至少一个数据分片包括需读取的数据块，和该数据块相应的元数据；对所述存储数据中的各数据分片进行逐片解压，如果解压过程中，确定数据分片中存在加密的数据块，根据该数据块的元数据选取解密算法，及确定网关连接的加密芯片提供的密钥；根据所述解密算法和密钥，对数据分片中存在加密的数据块进行解密；将数据分片解压后的未加密的数据块，和数据分片中解密的数据块相合并，得到读取数据；反馈所述读取数据给终端设备。

- 本申请实施例可利用私有云的网关所连接的加密芯片提供的密钥，对待存储数据的部分或全部进行加密，从而将包含加密后的密文的数据进行至公有云的存储；由于目标待存储数据包含以加密芯片提供的密钥所加密的密文，并且加密所使用的密钥由加密芯片存储，密钥泄露的风险极低，可降低由于云管理员泄露数据、公有云被黑客攻击等情况下的数据泄露风险，提升了私有云存储在公有云中的数据的安全性。

- 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的装置而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

专业人员还可以进一步意识到，结合本文中所公开的实施例描述的各示例的

单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

- 5 结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器 (RAM)、内存、只读存储器 (ROM)、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的
10 存储介质中。

- 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的核心思想或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。
- 15

权利要求书

- 1、一种混合云的数据存储方法，应用于私有云的网关，所述方法包括：
获取待存储数据；
从待存储数据中确定需加密的部分数据，得到第一目标数据；
5 获取所述第一目标数据进行加密后的第一密文；其中，根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密；
根据所述第一密文生成包含所述第一密文的第二目标数据；
根据所述第二目标数据生成所述第二目标数据对应的数据分片；
将所述第二目标数据对应的所述数据分片传输至公有云中存储。
- 10 2、根据权利要求1所述的混合云的数据存储方法，其中，所述从待存储数据中确定需加密的部分数据，得到第一目标数据包括：
确定待存储数据中需加密的部分数据的大小，以及确定需加密的部分数据在待存储数据中相应的位置；
根据所述大小和所述位置，从待存储数据中确定需加密的部分数据，并将所
15 述部分数据作为所述第一目标数据。
- 3、根据权利要求2所述的混合云的数据存储方法，其中，所述确定需加密的部分数据在待存储数据中相应的位置包括：
确定需加密的部分数据在待存储数据中相应的块内地址偏移；
所述根据所述第一密文生成包含所述第一密文的第二目标数据包括：
20 根据所述块内地址偏移，将所述第一密文覆盖到所述待存储数据中所述第一目标数据的原始位置，得到所述第二目标数据。
- 4、根据权利要求2所述的混合云的数据存储方法，其中，所述获取所述第一目标数据进行加密后的第一密文包括：
将所述第一目标数据传输至所连接的加密芯片；
25 从所述加密芯片获取所述第一密文，其中，所述加密芯片根据所存储的所述第一密钥，对所述目标数据进行加密以生成所述第一密文。
- 5、根据权利要求4所述的混合云的数据存储方法，进一步包括：
调取设置表格；
当所述设置表格指示由加密芯片进行加密时，触发执行所述将所述第一目标
30 数据传输至所连接的加密芯片的步骤。
- 6、根据权利要求5所述的混合云的数据存储方法，其中，所述确定待存储数据中需加密的部分数据的大小包括：
确定所述设置表格记录的待存储数据中需加密的部分数据的大小；
所述确定需加密的部分数据在待存储数据中相应的位置包括：
35 确定所述设置表格记录的需加密的部分数据在待存储数据中相应的位置。
- 7、根据权利要求5所述的混合云的数据存储方法，进一步包括：
若所述设置表格指示对待存储数据部分加密，触发执行所述从待存储数据中确定需加密的部分数据的步骤。
- 8、根据权利要求5所述的混合云的数据存储方法，进一步包括：
40 当所述设置表格指示对所述待存储数据进行全部加密，获取所述待存储数据进行加密后的第二密文；其中，根据所述网关所连接的加密芯片提供的第二密钥对所述待存储数据进行加密；

根据所述第二密文生成所述第二密文对应的数据分片，并传输至公有云中存储。

9、根据权利要求 8 所述的混合云的数据存储方法，其中，所述获取待存储数据进行加密后的第二密文包括：

5 判断上一次向所述加密芯片请求的所述第二密钥，是否处于设定的生命周期内；

当所述第二密钥，处于设定的生命周期内时，获取所述第二密钥，根据该第二密钥对所述待存储数据进行加密，得到第二密文；

10 如果所述第二密钥，不处于设定的生命周期内，向加密芯片请求第三密钥，根据请求得到的所述第三密钥对所述待存储数据进行加密，得到第二密文。

10、根据权利要求 1 所述的混合云的数据存储方法，进一步包括：

判断所获取的待存储数据的地址空间，是否与设置表格中记录的需加密的待存储数据的地址空间相对应；及根据设置表格中记录的需加密的待存储数据的存储频次，判断所获取的待存储数据是否需要加密；

15 如果判断结果均为是，触发执行所述从待存储数据中确定需加密的部分数据的步骤。

11、一种网关，包括：存储器和处理器，所述存储器存储有程序，所述处理器调用所述程序；所述程序用于执行如权利要求 1-10 任一项所述的方法。

20 12、一种存储介质，所述存储介质记录有程序，可以使至少一个处理器执行如权利要求 1-10 任一项所述的方法。

13、一种混合云的数据存储方法，应用于加密芯片，所述方法包括：

获取私有云的网关传输的待存储数据中需加密的目标数据；

根据密钥对所述目标数据进行加密，得到第一密文；

25 输出所述第一密文至所述网关，以便所述网关根据所述第一密文确定存储至公有云中的数据。

14、根据权利要求 13 所述的方法，其中，所述密钥是一组特定的秘密数据；

当加密时，所述密钥控制加密算法按照第一指定方式将明文变换为相应的密文，并将一组信源标识信息变换不可伪造的签名信息；

30 当解密时，所述密钥控制解密算法按照第二指定方式将所述密文变换为相应的所述明文，并将所述签名信息变换成所述信源标识信息。

15、一种加密芯片，包括：存储器和处理器，所述存储器存储有程序，所述处理器调用所述程序；所述程序用于执行如权利要求 13-14 任一项所述的方法。

35 16、一种存储介质，所述存储介质记录有程序，可以使至少一个处理器执行如权利要求 13-14 任一项所述的方法。

17、一种云系统，包括：位于私有云内的至少一个终端设备，网关，与所述网关连接的加密芯片；位于公有云内的存储转换服务器和存储设备；

其中，所述网关，用于获取待存储数据；从待存储数据中确定需加密的部分数据，得到第一目标数据；获取所述第一目标数据进行加密后的第一密文；其中，
40 根据所述网关所连接的加密芯片提供的第一密钥对所述第一目标数据进行加密；根据所述第一密文生成包含所述第一密文的第二目标数据；根据所述第二目标数据生成所述第二目标数据对应的数据分片；将所述第二目标数据对应的所述数据分片传输至公有云中存储；

所述存储转换服务器，用于根据所述数据分片生成存储数据，并将所述存储数据更新到存储设备上。

18、根据权利要求 17 所述的云系统，其中，所述网关确定待存储数据中需加密的部分数据的大小，以及确定需加密的部分数据在待存储数据中相应的位置；

5 根据所述大小和所述位置，从待存储数据中确定需加密的部分数据，并将所述部分数据作为所述第一目标数据。

19、根据权利要求 18 所述的云系统，其中，所述网关确定需加密的部分数据在待存储数据中相应的块内地址偏移；

10 所述网关并根据所述块内地址偏移，将所述第一密文覆盖到所述待存储数据中所述第一目标数据的原始位置，得到所述第二目标数据。

20、根据权利要求 18 所述的云系统，其中，所述网关将所述第一目标数据传输至所连接的加密芯片；

所述加密芯片根据所存储的所述第一密钥，对所述目标数据进行加密以生成所述第一密文；

15 所述网关，从所述加密芯片获取所述第一密文。

21、根据权利要求 20 所述的云系统，其中，所述网关，进一步调取设置表格；

当所述设置表格指示由加密芯片进行加密时，所述网关将所述第一目标数据传输至所述加密芯片。

20 22、根据权利要求 21 所述的云系统，其中，所述网关确定所述设置表格记录的待存储数据中需加密的部分数据的大小；

所述网关确定所述设置表格记录的需加密的部分数据在待存储数据中相应的位置。

25 23、根据权利要求 21 所述的云系统，其中，若所述设置表格指示对待存储数据部分加密，所述网关从待存储数据中确定需加密的部分数据。

24、根据权利要求 21 所述的云系统，其中，当所述设置表格指示对所述待存储数据进行全部加密，所述网关，获取所述待存储数据进行加密后的第二密文；其中，所述网关根据所述加密芯片提供的第二密钥对所述待存储数据进行加密；

30 所述网关根据所述第二密文生成所述第二密文对应的数据分片，并传输至所述存储转换服务器。

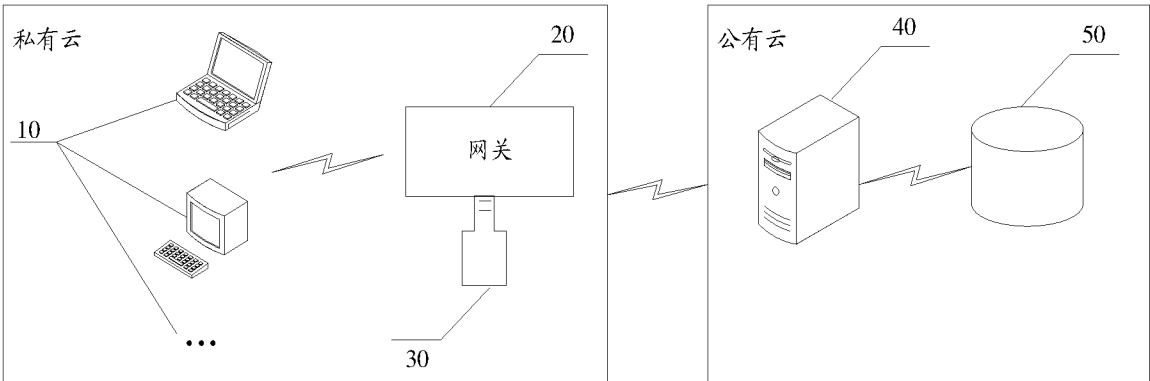


图 1

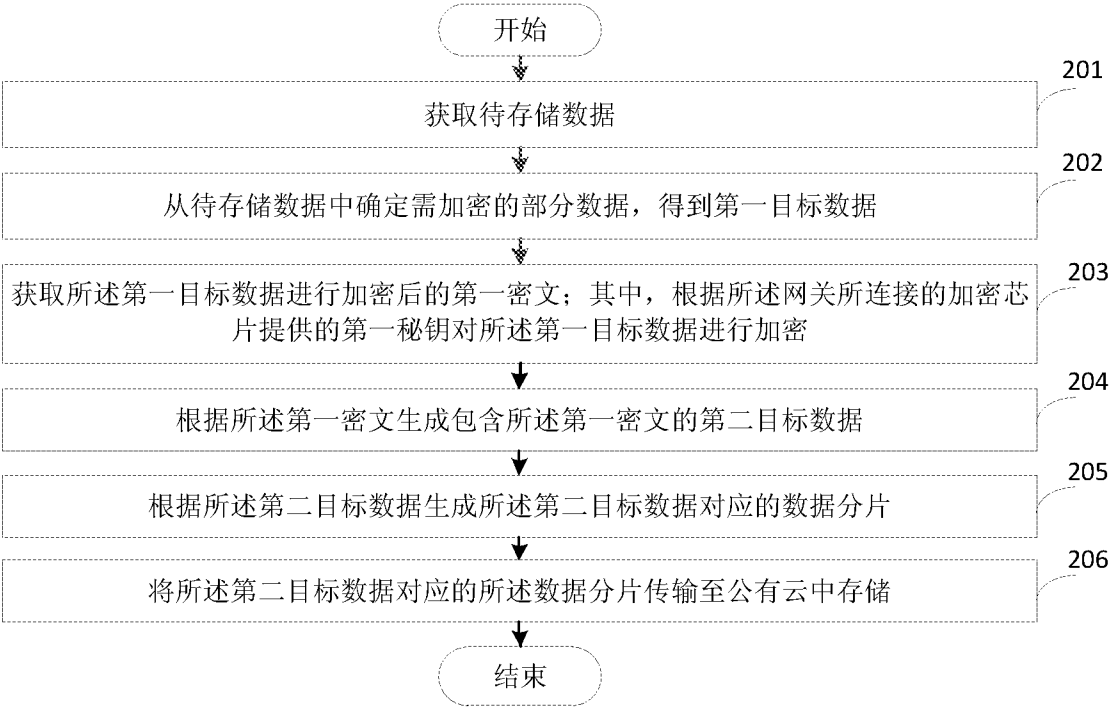


图 2A

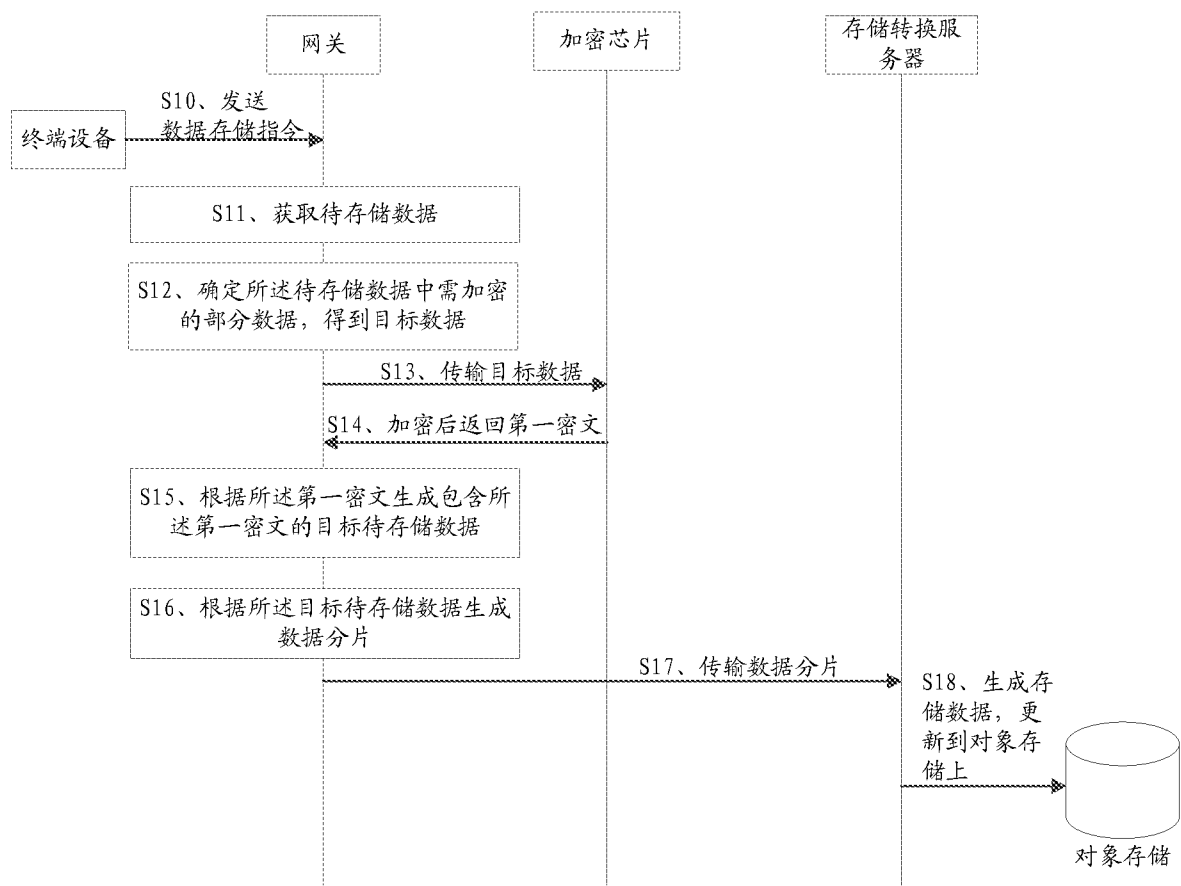


图 2B

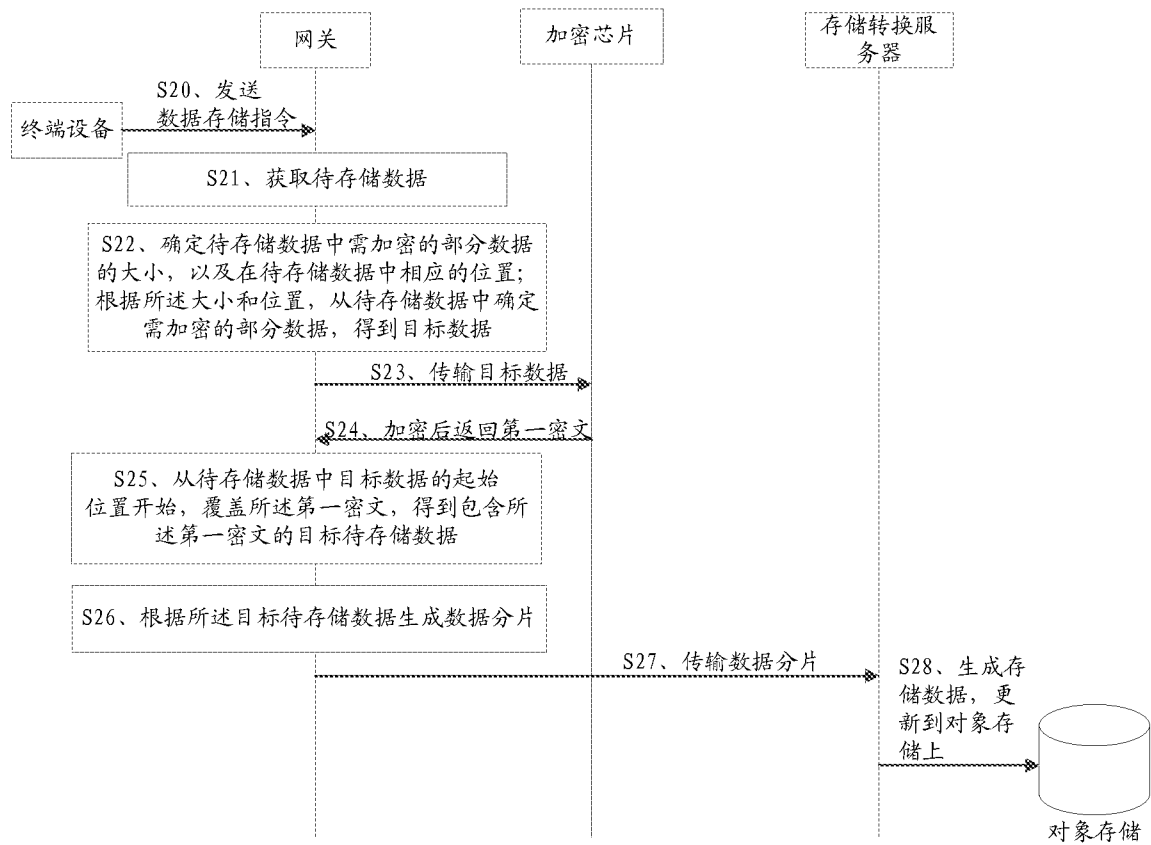


图 3

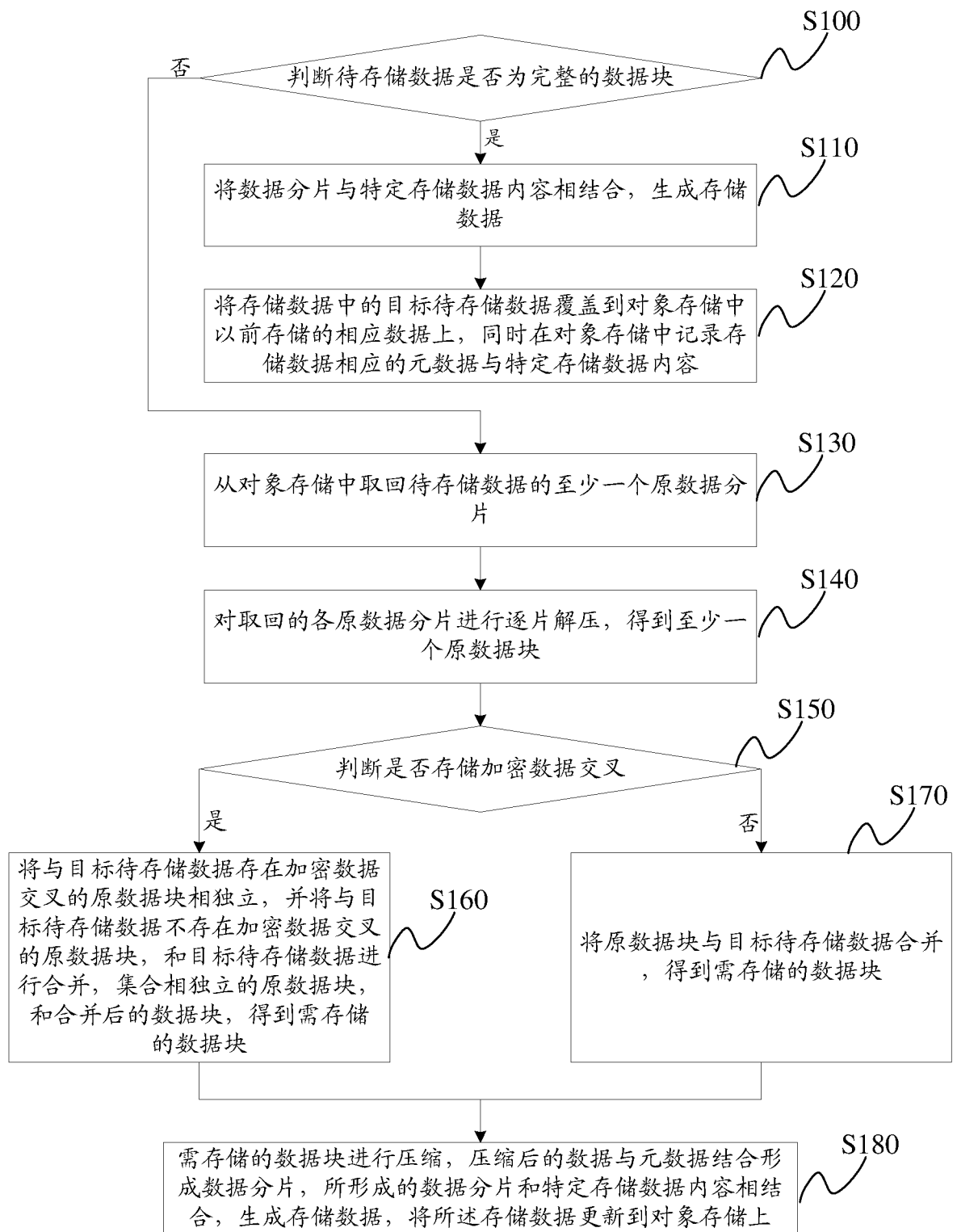


图 4

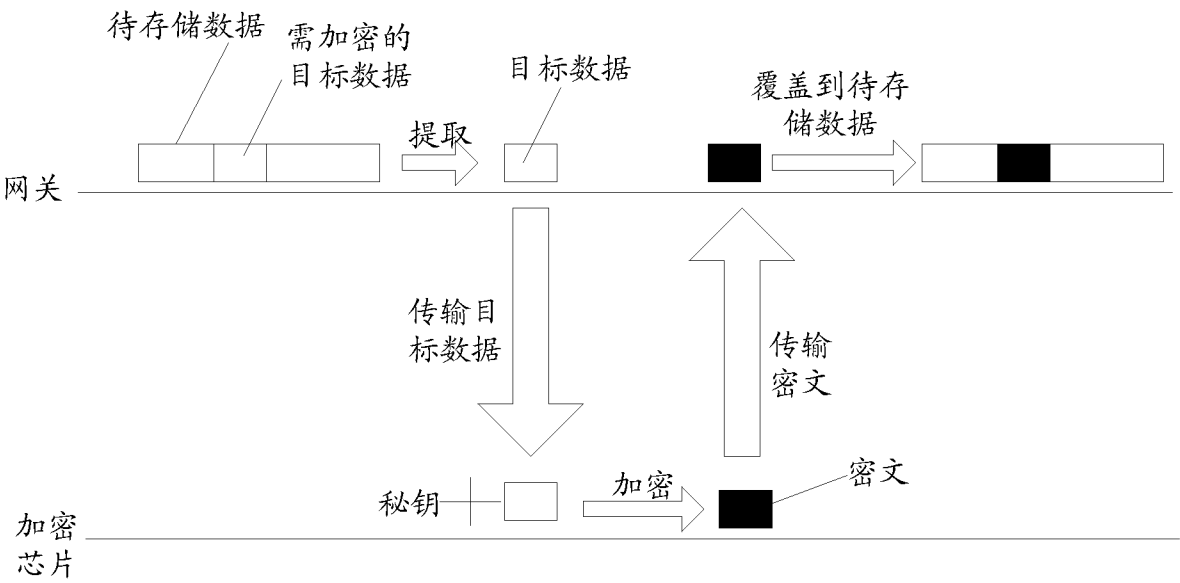


图 5

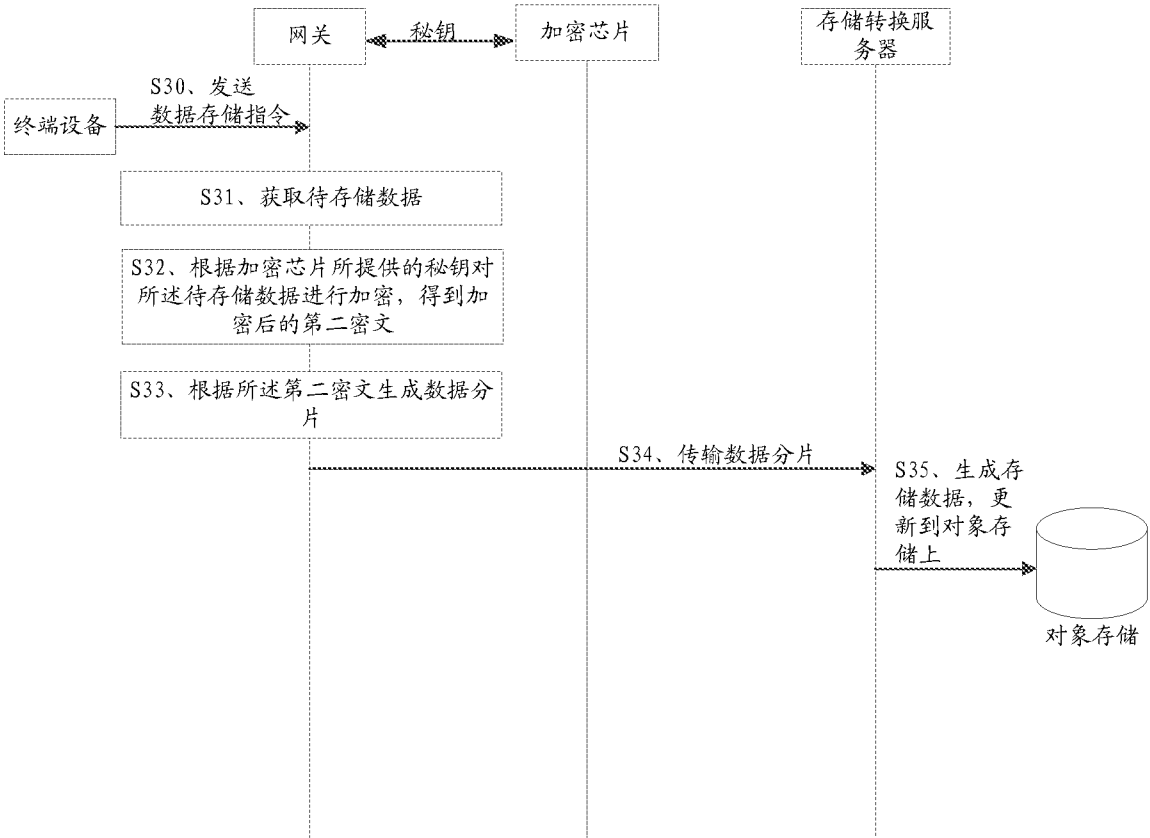


图 6

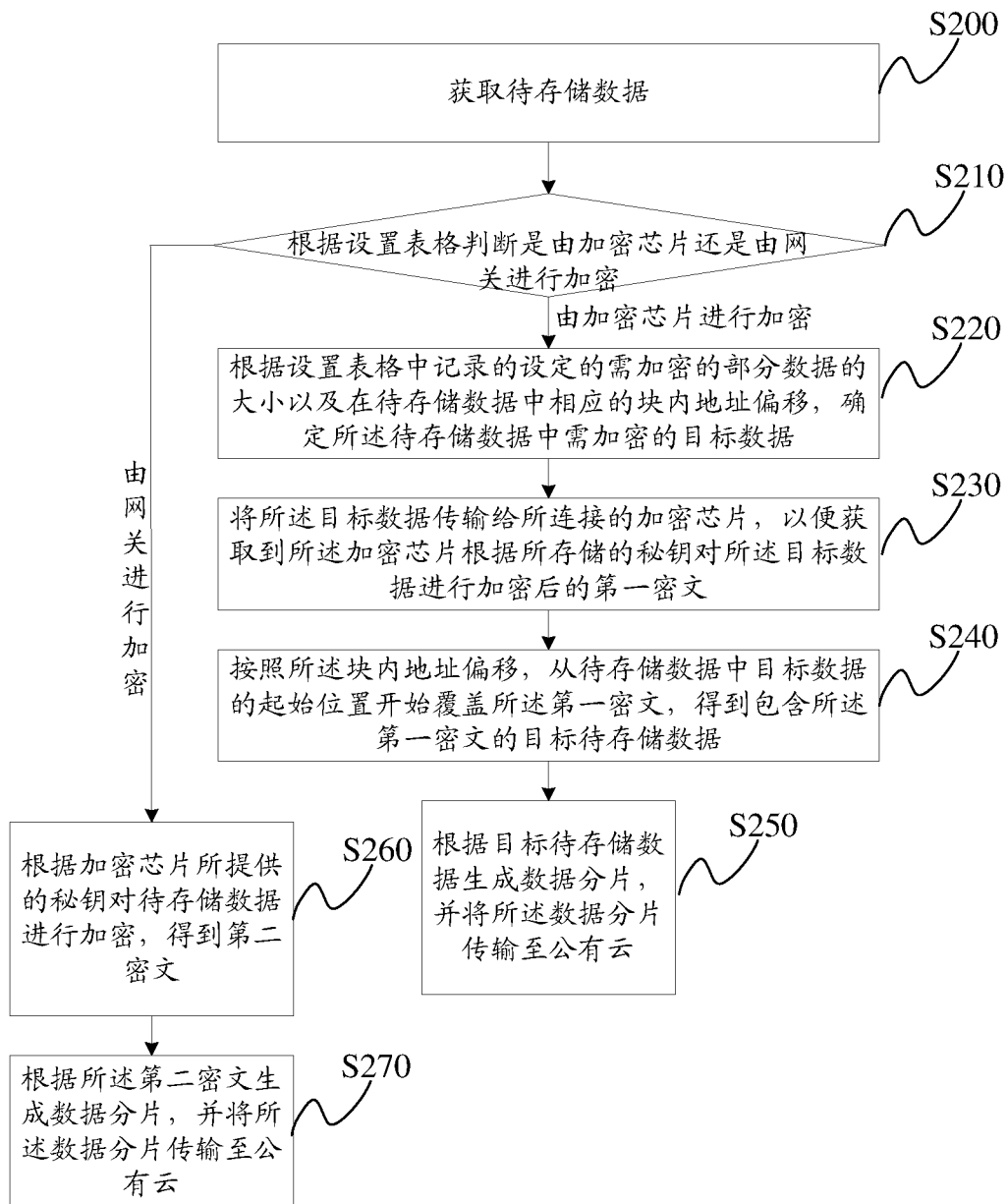


图 7

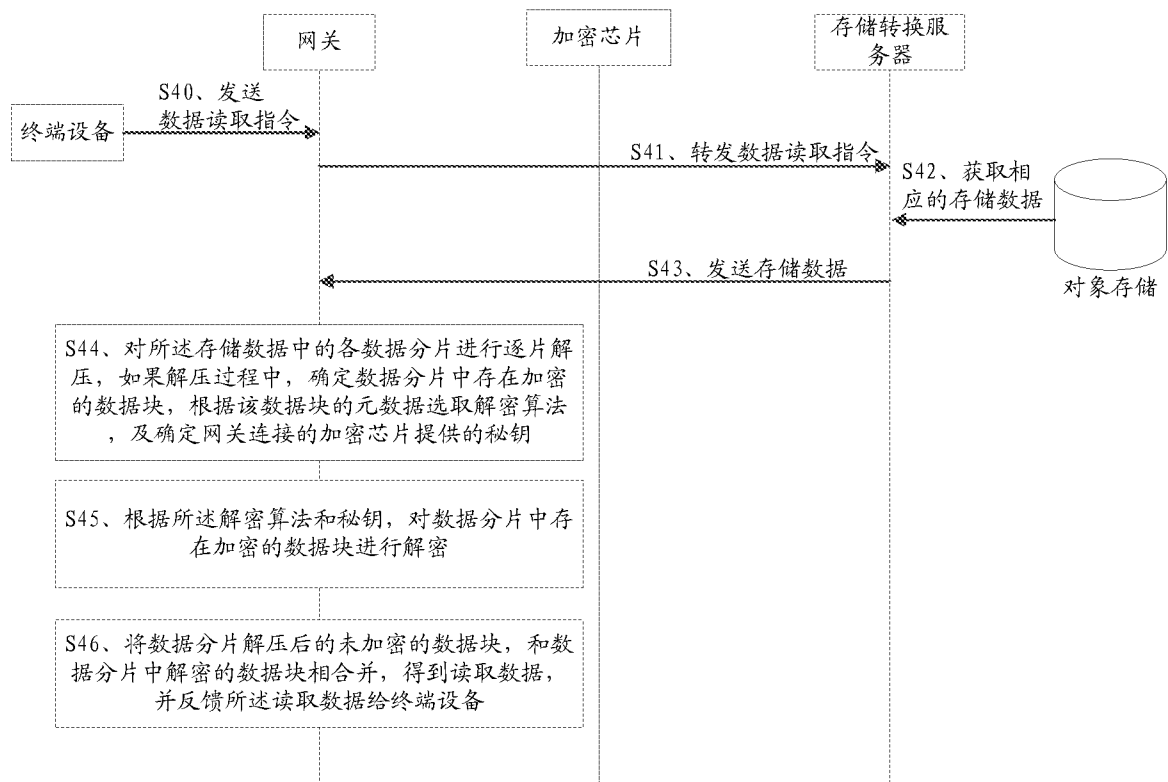


图 8

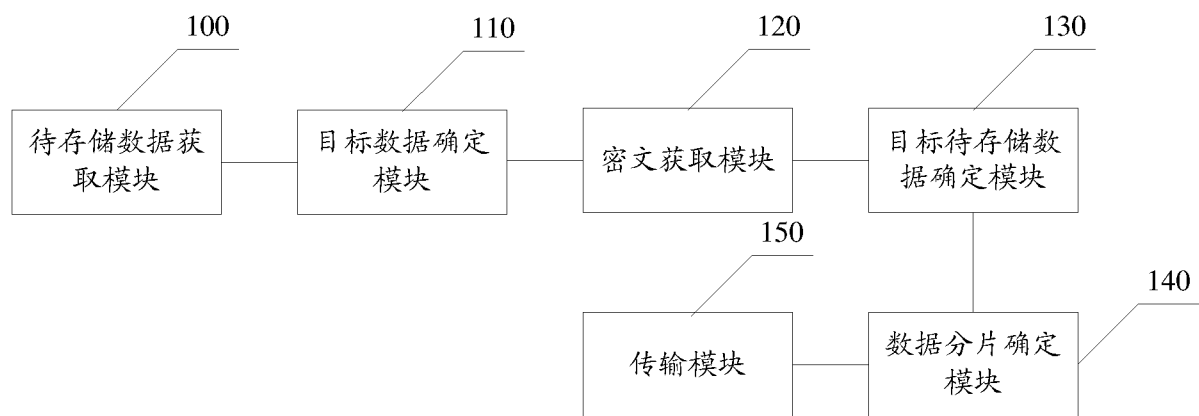


图 9

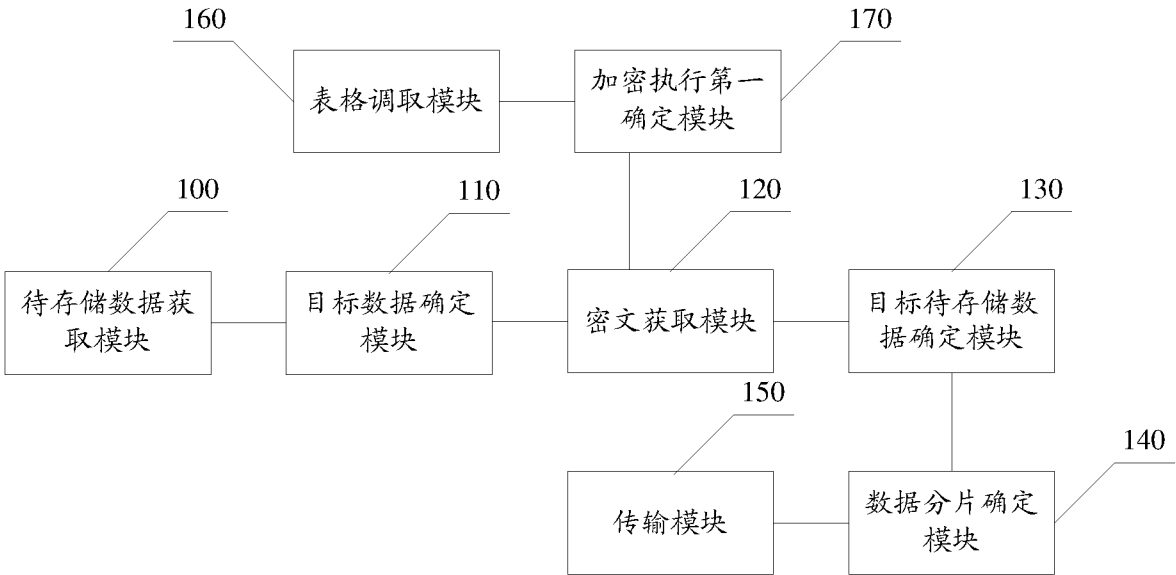


图 10

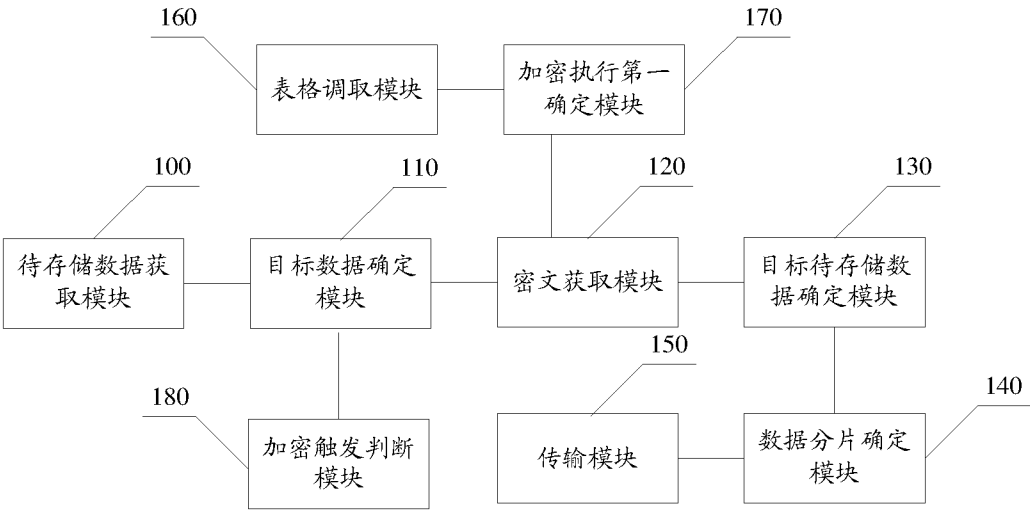


图 11

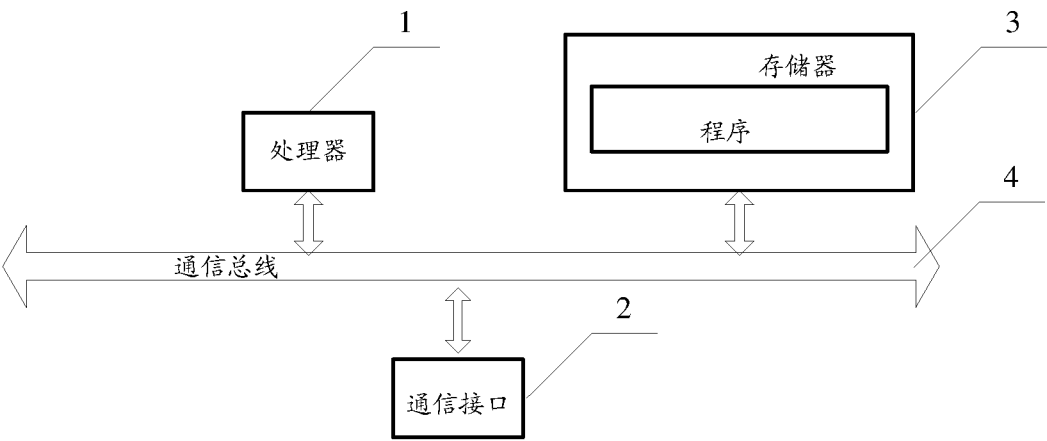


图 12

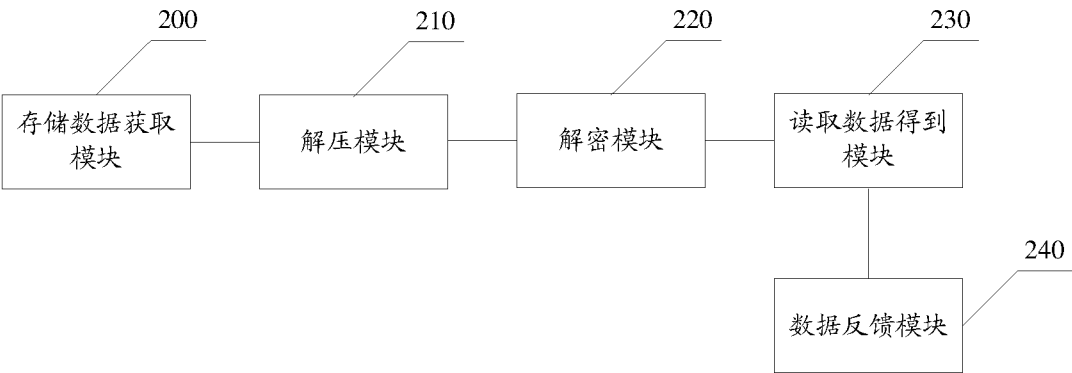


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/096072

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, GOOGLE: 混合云, 私有云, 公有云, 公共云, 数据, 存储, 网关, 加密, 传输, hybrid cloud, private cloud, public cloud, data, storage, gateway, encryption, transmission, cipher, safety

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107330337 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 07 November 2017 (2017-11-07) description, paragraphs 80-319	1-24
X	CN 106209823 A (XIDIAN UNIVERSITY) 07 December 2016 (2016-12-07) description, paragraphs 5-89	1-24
A	CN 105283879 A (CISCO TECHNOLOGY, INC.) 27 January 2016 (2016-01-27) entire document	1-24
A	CN 106100824 A (LIANSHAN PIPE CONTROLLED (BEIJING) INFORMATION TECHNOLOGY CO., LTD. ET AL.) 09 November 2016 (2016-11-09) entire document	1-24
A	US 2017026355 A1 (CISCO TECHNOLOGY, INC.) 26 January 2017 (2017-01-26) entire document	1-24
A	US 2016330177 A1 (CITRIX SYSTEMS, INC.) 10 November 2016 (2016-11-10) entire document	1-24



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

25 August 2018

Date of mailing of the international search report

26 September 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/096072

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107330337	A	07 November 2017	None			
CN	106209823	A	07 December 2016	None			
CN	105283879	A	27 January 2016	WO	2014200778	A1	18 December 2014
				EP	3008657	A1	20 April 2016
				US	2014366155	A1	11 December 2014
CN	106100824	A	09 November 2016	None			
US	2017026355	A1	26 January 2017	None			
US	2016330177	A1	10 November 2016	WO	2016183066	A1	17 November 2016
				EP	3295642	A1	21 March 2018

国际检索报告

国际申请号

PCT/CN2018/096072

A. 主题的分类

G06F 21/60(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, WPI, EPODOC, CNKI, GOOGLE: 混合云, 私有云, 公有云, 公共云, 数据, 存储, 网关, 加密, 传输, hybrid cloud, private cloud, public cloud, data, storage, gateway, encryption, transmission, cipher, safety

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 107330337 A (腾讯科技深圳有限公司) 2017年 11月 7日 (2017 - 11 - 07) 说明书第80-319段	1-24
X	CN 106209823 A (西安电子科技大学) 2016年 12月 7日 (2016 - 12 - 07) 说明书第5-89段	1-24
A	CN 105283879 A (思科技术公司) 2016年 1月 27日 (2016 - 01 - 27) 全文	1-24
A	CN 106100824 A (连山管控北京信息技术有限公司等) 2016年 11月 9日 (2016 - 11 - 09) 全文	1-24
A	US 2017026355 A1 (CISCO TECHNOLOGY, INC.) 2017年 1月 26日 (2017 - 01 - 26) 全文	1-24
A	US 2016330177 A1 (CITRIX SYSTEMS, INC.) 2016年 11月 10日 (2016 - 11 - 10) 全文	1-24

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2018年 8月 25日

国际检索报告邮寄日期

2018年 9月 26日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

白雪慧

电话号码 86-(10)-53961635

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/096072

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107330337	A	2017年 11月 7日	无			
CN	106209823	A	2016年 12月 7日	无			
CN	105283879	A	2016年 1月 27日	WO	2014200778	A1	2014年 12月 18日
				EP	3008657	A1	2016年 4月 20日
				US	2014366155	A1	2014年 12月 11日
CN	106100824	A	2016年 11月 9日	无			
US	2017026355	A1	2017年 1月 26日	无			
US	2016330177	A1	2016年 11月 10日	WO	2016183066	A1	2016年 11月 17日
				EP	3295642	A1	2018年 3月 21日

表 PCT/ISA/210 (同族专利附件) (2015年1月)