(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 117527193 B
(45)授权公告日 2024.07.16

(21)申请号 202311373479.9
(22)申请日 2023.10.20
(65)同一申请的已公布的文献号
申请公布号 CN 117527193 A
(43)申请公布日 2024.02.06
(73)专利权人 合芯科技有限公司
地址 510799 广东省广州市黄埔区瑞吉二街45号101、301房
专利权人 合芯科技(苏州)有限公司
(72)发明人 陶传会
(74)专利代理机构 北京三聚阳光知识产权代理有限公司 11250
专利代理师 刘静
(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 69/06(2022.01)
(56)对比文件
CN 113779619 A,2021.12.10
审查员 何花

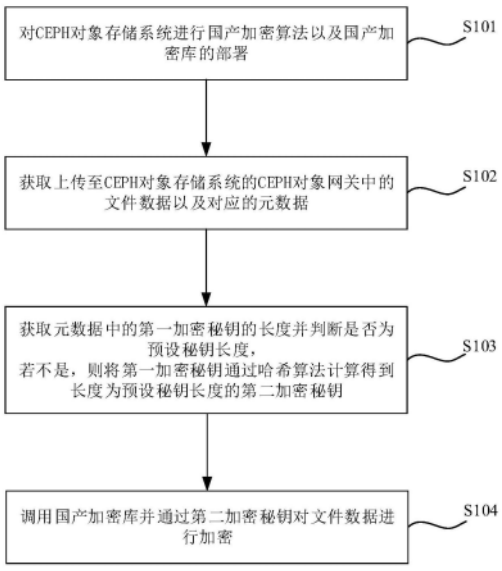
权利要求书2页 说明书10页 附图6页

(54)发明名称

一种基于国密CEPH对象存储的加密方法及装置

(57)摘要

本发明涉及数据存储加密技术领域,公开了一种基于国密CEPH对象存储的加密方法及装置,方法包括:对CEPH对象存储系统进行国产加密算法及国产加密库的部署;获取CEPH对象网关中的文件数据以及对应的元数据;获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥;调用国产加密库并通过第二加密秘钥对文件数据。使用国产的加密算法和加密库,可以确保数据的加密过程符合国内的加密标准,无需适配国外的加密标准,有效保护CEPH对象存储系统中的数据,避免数据受到潜在的安全威胁,提高了数据安全性。



CN 117527193 B

1.一种基于国密CEPH对象存储的加密方法,应用于CEPH对象存储系统,其特征在于,所述方法包括:

对CEPH对象存储系统进行国产加密算法以及国产加密库的部署;

获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据;

获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,所述预设秘钥长度为国产加密算法对应的秘钥长度;其中,所述将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥的步骤包括:对第一加密秘钥通过哈希算法计算得到的预设位数的哈希值,从索引位置为零开始,截取长度为预设个数的子串作为新的秘钥,即第二加密秘钥,或者,对第一加密秘钥通过哈希算法计算得到的预设位数的哈希值,从索引位置为零开始,每隔一个索引位置的值进行提取,得到预设个数的子串作为新的秘钥,即第二加密秘钥;

调用国产加密库并通过第二加密秘钥对文件数据进行加密。

2.根据权利要求1所述的方法,其特征在于,所述对CEPH对象存储系统进行国产加密算法以及国产加密库的部署,包括:

将CEPH对象网关的源代码中加密算法设置为国密算法;

将CEPH对象网关的源代码中加密插件中的默认加密库设置为国产加密库;

编译CEPH对象网关源代码,成功编译后对CEPH对象存储系统进行基本部署。

3.根据权利要求2所述的方法,其特征在于,所述将CEPH对象网关的源代码中加密插件中的默认加密库设置为国产加密库,包括:

将CEPH对象网关的源代码中默认加密库的加密函数修改为国产加密库对应的加密函数;

将CEPH对象网关的模块中默认加密库的命名修改为国产加密库的命名。

4.根据权利要求1所述的方法,其特征在于,所述方法,还包括:

若是,则将第一加密秘钥直接设置为第二加密秘钥。

5.根据权利要求1所述的方法,其特征在于,所述调用国产加密库并通过第二加密秘钥对文件数据进行加密之前,还包括:

基于CEPH对象存储系统支持的格式对原始的文件数据进行格式处理,得到处理后的文件数据。

6.根据权利要求5所述的方法,其特征在于,所述调用国产加密库并通过第二加密秘钥对文件数据进行加密,包括:

基于CEPH对象存储系统的配置文件获取配置信息;

判断所述配置信息中指定路径下是否配置外部加密引擎,若存在,则通过国产加密库使用外部加密引擎接口调用外置加密卡对文件数据进行加密;若不存在,则调用国产加密库使用CEPH对象存储系统内置算法对文件数据进行加密。

7.根据权利要求1至6中任一项所述的方法,其特征在于,所述调用国产加密库并通过第二加密秘钥对文件数据进行加密之后,还包括:

获取生成的密文数据,并对所述密文数据进行验证;

创建CEPH对象加密存储桶,将验证通过后的密文数据存储至所述CEPH对象加密存储

桶。

8.一种基于国密CEPH对象存储的加密装置,其特征在于,所述装置包括:

配置及部署模块,用于对CEPH对象存储系统进行国产加密算法以及国产加密库的部署;

数据获取模块,用于获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据;

秘钥计算模块,用于获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,所述预设秘钥长度为国产加密算法对应的秘钥长度;其中,所述将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥的步骤包括:对第一加密秘钥通过哈希算法计算得到的预设位数的哈希值,从索引位置为零开始,截取长度为预设个数的子串作为新的秘钥,即第二加密秘钥,或者,对第一加密秘钥通过哈希算法计算得到的预设位数的哈希值,从索引位置为零开始,每隔一个索引位置的值进行提取,得到预设个数的子串作为新的秘钥,即第二加密秘钥;

国产加密模块,用于调用国产加密库并通过第二加密秘钥对文件数据进行加密。

9.一种计算机设备,其特征在于,包括:

存储器和处理器,所述存储器和所述处理器之间互相通信连接,所述存储器中存储有计算机指令,所述处理器通过执行所述计算机指令,从而执行权利要求1至7中任一项所述的基于国密CEPH对象存储的加密方法。

10.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有计算机指令,所述计算机指令用于使计算机执行权利要求1至7中任一项所述的基于国密CEPH对象存储的加密方法。

一种基于国密CEPH对象存储的加密方法及装置

技术领域

[0001] 本发明涉及数据存储加密技术领域,具体涉及一种基于国密CEPH对象存储的加密方法及装置。

背景技术

[0002] 随着互联网技术高速发展,海量数据存储需求迅速增加。在这样的环境下,CEPH(分布式存储系统)应运而生,并且通过提供多种数据存储形式和具备稳定性、高可用性和海量数据存储等方面的优势而受到广泛关注。

[0003] 随着用户对数据安全的日益重视,CEPH在部分存储分支(如对象存储和块存储)中引入了数据加密功能,然而,CEPH中数据加密功能使用的加密算法是其他国家提出的AES加密标准(高级加密标准)。尽管AES加密标准被广泛认可,在国内的企业级应用中,依赖其他国家提出的CEPH的加密功能存在潜在的安全威胁,并无法完全保证数据安全性。

发明内容

[0004] 有鉴于此,本发明提供了一种基于国密CEPH对象存储的加密方法及装置,以解决在国内使用CEPH的加密功能时数据安全性不高的问题。

[0005] 第一方面,本发明提供了一种基于国密CEPH对象存储的加密方法,方法包括:对CEPH对象存储系统进行国产加密算法以及国产加密库的部署;获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据;获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,所述预设秘钥长度为国产加密算法对应的秘钥长度;调用国产加密库并通过第二加密秘钥对文件数据进行加密。

[0006] 本发明实施例通过部署国产加密算法和加密库,确保使用的是符合国家标准的加密算法和库。获取元数据中的第一加密秘钥的长度,并判断是否与预设秘钥长度相同。如果不相同,将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,保证秘钥为国产加密算法对应的秘钥。调用国产加密库,使用第二加密秘钥对文件数据进行加密。使用国产的加密算法和加密库,可以确保数据的加密过程符合国内的加密标准,无需适用国外的加密标准,有效保护CEPH对象存储系统中的数据,避免数据受到潜在的安全威胁,提高了数据安全性。

[0007] 在一种可选的实施方式中,所述对CEPH对象存储系统进行国产加密算法以及国产加密库的部署,包括:将CEPH对象网关的源代码中加密算法设置为国密算法;将CEPH对象网关的源代码中加密插件中的默认加密库设置为国产加密库;编译CEPH对象网关源代码,成功编译后对CEPH对象存储系统进行基本部署。

[0008] 通过将CEPH对象网关源代码中的算法设置为国产加密算法,将默认加密库修改为国产加密库,确保对CEPH对象存储系统中的数据更加安全,使用国密算法作为对象存储的密码学对称加密算法,替代了原有的国外标准算法,满足国内的加密法规和法律要求,并提

高数据的机密性和完整性。

[0009] 在一种可选的实施方式中,所述将CEPH对象网关的源代码中加密插件中的默认加密库设置为国产加密库,包括:将CEPH对象网关的源代码中默认加密库的加密函数修改为国产加密库对应的加密函数;将CEPH对象网关的模块中默认加密库的命名修改为国产加密库的命名。

[0010] 通过将CEPH对象网关的源代码中加密插件的默认加密库设置为国产加密库,包括修改加密函数和命名调整,在更新时更加方便快捷,平滑兼容,无需修改全部代码,同时使用国产加密库减少对国外加密库的依赖。

[0011] 在一种可选的实施方式中,所述方法,还包括:若是,则将第一加密秘钥直接设置为第二加密秘钥。

[0012] 通过获取元数据中的第一加密秘钥长度并判断是否达到预设秘钥长度,若达不到,则对秘钥进行哈希运算,确保秘钥长度达到国产加密算法标准,若达到预设秘钥长度,则第一加密秘钥符合加密标准,为后续加密操作提供数据基础。

[0013] 在一种可选的实施方式中,所述调用国产加密库并通过第二加密秘钥对文件数据进行加密之前,还包括:基于CEPH对象存储系统支持的格式对原始的文件数据进行格式处理,得到处理后的文件数据。

[0014] 通过基于CEPH对象存储系统支持的格式对原始文件数据进行处理,保证了数据的格式统一,从而提高了数据的可读性和可操作性。

[0015] 在一种可选的实施方式中,所述调用国产加密库并通过第二加密秘钥对文件数据进行加密,包括:基于CEPH对象存储系统的配置文件获取配置信息;判断所述配置信息中指定路径下是否配置外部加密引擎,若存在,则通过国产加密库使用外部加密引擎接口调用外置加密卡对文件数据进行加密;若不存在,则调用国产加密库使用CEPH对象存储系统内置算法对文件数据进行加密。

[0016] 通过调用国产加密库并根据配置信息判断是否使用外部加密引擎,实现了灵活的加密方式选择。若配置中存在外部加密引擎,则通过国产加密库调用外置加密卡对文件数据进行加密,提高了加密效率,若不存在外部加密引擎,则使用CEPH对象存储系统内置算法进行加密,确保数据的安全性。提供外置国密加密卡的功能及实现方案,从而极大提高系统内部对数据加密的算力和可信度。

[0017] 在一种可选的实施方式中,所述调用国产加密库并通过第二加密秘钥对文件数据进行加密之后,还包括:获取生成的密文数据,并对所述密文数据进行验证;创建CEPH对象加密存储桶,将验证通过后的密文数据存储至所述CEPH对象加密存储桶。

[0018] 通过获取生成的密文数据并进行验证,并创建CEPH对象加密存储桶将验证通过的密文数据存储其中,实现对加密数据的集中存储,从而确保加密后的数据完整性。

[0019] 第二方面,本发明提供了一种基于国密CEPH对象存储的加密装置,所述装置包括:

[0020] 配置及部署模块,用于对CEPH对象存储系统进行国产加密算法以及国产加密库的部署;

[0021] 数据获取模块,用于获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据;

[0022] 秘钥计算模块,用于获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥

长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,所述预设秘钥长度为国产加密算法对应的秘钥长度;

[0023] 国产加密模块,用于调用国产加密库并通过第二加密秘钥对文件数据进行加密。

[0024] 第三方面,本发明提供了一种计算机设备,包括:存储器和处理器,存储器和处理器之间互相通信连接,存储器中存储有计算机指令,处理器通过执行计算机指令,从而执行上述第一方面或其对应的任一实施方式的基于国密CEPH对象存储的加密方法。

[0025] 第四方面,本发明提供了一种计算机可读存储介质,该计算机可读存储介质上存储有计算机指令,计算机指令用于使计算机执行上述第一方面或其对应的任一实施方式的基于国密CEPH对象存储的加密方法。

附图说明

[0026] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案,下面将对具体实施方式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,下面描述中的附图是本发明的一些实施方式,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,还可以根据这些附图获得其他的附图。

[0027] 图1是根据本发明实施例的基于国密CEPH对象存储的加密方法的流程示意图;

[0028] 图2是根据本发明实施例的另一基于国密CEPH对象存储的加密方法的流程示意图;

[0029] 图3是根据本发明实施例的另一基于国密CEPH对象存储的加密方法的流程示意图;

[0030] 图4是根据本发明实施例的另一基于国密CEPH对象存储的加密方法的流程示意图;

[0031] 图5是根据本发明实施例的另一基于国密CEPH对象存储的加密方法的流程示意图;

[0032] 图6是根据本发明实施例的基于国密CEPH对象存储的加密装置的模块组成示意图;

[0033] 图7是本发明实施例的计算机设备的硬件结构示意图。

具体实施方式

[0034] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。

[0035] 基于本发明中的实施例,本领域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,都属于本发明保护的范围。

[0036] 根据本发明实施例,提供了一种基于国密CEPH对象存储的加密方法实施例,需要说明的是,在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行,并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0037] 在本实施例中提供了一种基于国密CEPH对象存储的加密方法,可用于上述的计算

机设备,应用于CEPH对象存储系统,图1是根据本发明实施例的基于国密CEPH对象存储的加密方法的流程图,如图1所示,该流程包括如下步骤:

[0038] 步骤S101,对CEPH对象存储系统进行国产加密算法以及国产加密库的部署。

[0039] 本发明实施例中,CEPH对象存储系统指的是一种分布式存储系统,用于存储和管理大规模的数据,由对象网关、存储集群和管理节点组成。国产加密算法的部署指的是将国内开发的加密算法集成到CEPH对象存储系统中,用于对存储的数据进行加密和解密操作。国产加密库的部署则是指将国内开发的加密库集成到CEPH对象存储系统中。从而保证从加密库到加密算法全部采用国产技术,减少对国外加密技术的依赖。

[0040] 具体实现中,在CEPH对象存储系统的配置文件中配置国产加密算法,获取国产加密库的包,通过安装指示进行安装,编译config文件,将加密配置项设置为使用国产加密库,当再次启动CEPH服务后,加密库和加密算法的更改已经生效。

[0041] 步骤S102,获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据。

[0042] 本发明实施例中,CEPH对象网关中的文件数据指的是用户上传至CEPH对象存储系统的文件内容,例如文档、图片等,对应的元数据是与文件相关的描述信息,例如文件名、存储位置、文件大小、文件类型、创建时间等,获取CEPH对象网关中的文件数据以及对应的元数据可以方便后续利用国密算法对数据进行加密。

[0043] 可以理解的是,客户端使用对象存储协议与CEPH对象存储网关建立连接,想要上传txt文件(文件数据),并对其进行加密,则需要将要上传的txt文件进行分片处理,并按照指定顺序将分片上传到CEPH对象存储网关中,相关信息(元数据)中就存在相应的加密标志以及秘钥key。此时CEPH对象网关中已经包含有文件数据以及对应的元数据。

[0044] 步骤S103,获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,预设秘钥长度为国产加密算法对应的秘钥长度。

[0045] 本发明实施例中,第一加密秘钥指的是元数据中的原始秘钥。预设秘钥长度指的是能够满足加密算法要求的秘钥长度,第二加密秘钥指的是满足加密算法要求的秘钥。

[0046] 具体实现中,若第一加密秘钥的长度为256比特,而预设秘钥长度为128比特(对应SM4算法)。判断秘钥长度为256比特,不符合预设秘钥长度。使用哈希算法对第一加密秘钥进行计算,得到长度为128比特的第二加密秘钥key-2。计算方法可以是对哈希算法(例如SHA-256)计算后得到的256位哈希值,从索引位置0开始,截取长度为16的子串作为新的128位秘钥key-2;也可以是对哈希算法计算后得到的256位哈希值的每隔一个索引位置的值进行提取,取出的16个字符组成新的128位秘钥key-2。

[0047] 步骤S104,调用国产加密库并通过第二加密秘钥对文件数据进行加密。

[0048] 本发明实施例中,可以理解的是,通过对文件数据进行加密,以使在解密时检查数据是否被篡改过,提供数据完整验证。如果解密后的数据与加密前的数据不一致,说明数据可能已被篡改。调用国产加密库可以确保加密算法符合国家标准,并且经过了国家安全审计认证,不依赖国外加密库,保证数据的安全性。

[0049] 本发明实施例通过部署国产加密算法和加密库,确保使用的是符合国家标准的加密算法和库。获取元数据中的第一加密秘钥的长度,并判断是否与预设秘钥长度相同。如果

不相同,将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,保证秘钥为国产加密算法对应的秘钥。调用国产加密库,使用第二加密秘钥对文件数据进行加密。使用国产的加密算法和加密库,可以确保数据的加密过程符合国内的加密标准,无需适用国外的加密标准,有效保护CEPH对象存储系统中的数据,避免数据受到潜在的安全威胁,提高了数据安全性。

[0050] 在本实施例中提供了一种基于国密CEPH对象存储的加密方法,可用于上述的计算机等,图2是根据本发明实施例的基于国密CEPH对象存储的加密方法的流程图,如图2所示,该流程包括如下步骤:

[0051] 步骤S201,对CEPH对象存储系统进行国产加密算法以及国产加密库的部署。具体的,上述步骤S201包括:

[0052] 步骤S2011,将CEPH对象网关的源代码中加密算法设置为国密算法。

[0053] 示例性的,在CEPH对象网关的源代码中,找到负责加密的模块或函数,将原有的加密算法替换为符合国密标准的算法(例如是SM4算法)。修改SM4算法的代码逻辑,确保加密过程使用了国密算法进行加密操作。

[0054] 步骤S2012,将CEPH对象网关的源代码中加密插件中的默认加密库设置为国产加密库。

[0055] 本实施例中,在CEPH对象网关的源代码中,找到负责加密插件的相关模块或函数,将原有的默认加密库(例如是OpenSSL库)替换为国产加密库(例如是GmSSL)。

[0056] 进一步的,步骤S2012包括:

[0057] a1:将CEPH对象网关的源代码中默认加密库的加密函数修改为国产加密库对应的加密函数。

[0058] 示例性的,原本CEPH对象存储系统中使用了OpenSSL的加密函数openssl()来进行数据加密。将这些地方改为使用GmSSL的加密函数gmssl()。

[0059] a2:将CEPH对象网关的模块中默认加密库的命名修改为国产加密库的命名。

[0060] 示例性的,原本CEPH的一个模块依赖了OpenSSL库的名称为libssl.so和libcrypto.so,本发明实施例将GmSSL编译后的库名称修改为libgmssl.so和libgmcrypto.so。

[0061] 步骤S2013,编译CEPH对象网关源代码,成功编译后对CEPH对象存储系统进行基本部署。

[0062] 示例性的,在源代码目录保存后,执行编译命令编译CEPH对象网关源代码,等待编译过程完成,如果没有错误或警告信息,则表示编译成功。成功后部署CEPH对象存储系统,参照官方部署指南例如配置和启动CEPH集群、创建存储池等。

[0063] 对于本实施例,通过将CEPH对象网关的源代码中加密插件的默认加密库设置为国产加密库,包括修改加密函数和命名调整,在更新时更加方便快捷,平滑兼容,无需修改全部代码,同时使用国产加密库减少对国外加密库的依赖。

[0064] 步骤S202,获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据。详细请参见图1所示实施例的步骤S102,在此不再赘述。

[0065] 步骤S203,获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,预

设秘钥长度为国产加密算法对应的秘钥长度。详细请参见图1所示实施例的步骤S103,在此不再赘述。

[0066] 步骤S204,调用国产加密库并通过第二加密秘钥对文件数据进行加密。详细请参见图1所示实施例的步骤S104,在此不再赘述。

[0067] 对于本实施例,通过将CEPH对象网关源代码中的算法设置为国产加密算法,将默认加密库修改为国产加密库,确保对CEPH对象存储系统中的数据更加安全,使用国密算法作为对象存储的密码学对称加密算法,替代了原有的国外标准算法,满足国内的加密法规和法律要求,并提高数据的机密性和完整性。

[0068] 在本实施例中提供了一种基于国密CEPH对象存储的加密方法,可用于上述的计算机等,图3是根据本发明实施例的基于国密CEPH对象存储的加密方法的流程图,如图3所示,该流程包括如下步骤:

[0069] 步骤S301,对CEPH对象存储系统进行国产加密算法以及国产加密库的部署。详细请参见图1所示实施例的步骤S101,在此不再赘述。

[0070] 步骤S302,获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据。详细请参见图1所示实施例的步骤S102,在此不再赘述。

[0071] 步骤S303,获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,预设秘钥长度为国产加密算法对应的秘钥长度。详细请参见图1所示实施例的步骤S103,在此不再赘述。

[0072] 步骤S304,基于CEPH对象存储系统支持的格式对原始的文件数据进行格式处理,得到处理后的文件数据。

[0073] 本发明实施例中,可以理解的是处理原始的文件数据是为了适应CEPH对象存储系统的要求,满足CEPH对象存储系统的支持,例如将文本文件转换为JSON格式。

[0074] 对于本实施例,通过基于CEPH对象存储系统支持的格式对原始文件数据进行处理,基于CEPH对象存储系统支持的路径对元数据进行转换,以使元数据与系统的路径规则相匹配,保证了数据的格式统一。从而提高了数据的可读性和可操作性。

[0075] 步骤S305,调用国产加密库并通过第二加密秘钥对文件数据进行加密。详细请参见图1所示实施例的步骤S104,在此不再赘述。

[0076] 具体的,上述步骤S305包括:

[0077] 步骤S3051,基于CEPH对象存储系统的配置文件获取配置信息。

[0078] 可以理解的是,在CEPH对象存储系统的配置文件中,预先定义了配置信息,例如加密引擎的路径、加密算法的选择等。通过读取配置文件,获取这些配置信息,并在后续的步骤中使用。

[0079] 步骤S3052,判断配置信息中指定路径下是否配置外部加密引擎,若存在,则通过国产加密库使用外部加密引擎接口调用外置加密卡对文件数据进行加密;若不存在,则调用国产加密库使用CEPH对象存储系统内置算法对文件数据进行加密。

[0080] 需要说明的是,外部加密引擎指的是外置加密卡所提供的加密功能接口,用于与加密库进行通信和进行加密操作。外置加密卡指的是硬件设备,可以使插入式卡或模块,用于进行加密和解密操作,提供高级别的加密算法和性能加速,外置加密卡具有独立的密钥

管理和加密引擎,可以与加密库进行集成。通过使用外部加密卡和外部加密引擎,在保证机密性和安全性的同时,提供更高的加密性能和性能加速

[0081] 示例性的,在配置文件中查找指定路径下是否存在外部加密引擎的配置。如果存在外部加密引擎的配置,说明用户希望使用外置加密卡进行加密操作;如果不存在外部加密引擎的配置,则说明用户希望使用CEPH对象存储系统内置的加密算法进行加密操作。

[0082] 对于本实施例,通过调用国产加密库并根据配置信息判断是否使用外部加密引擎,实现了灵活的加密方式选择。若配置中存在外部加密引擎,则通过国产加密库调用外置加密卡对文件数据进行加密,提高了加密效率,若不存在外部加密引擎,则使用CEPH对象存储系统内置算法进行加密,确保数据的安全性。提供外置国密加密卡的功能及实现方案,从而极大提高系统内部对数据加密的算力和可信度。

[0083] 在本实施例中提供了一种基于国密CEPH对象存储的加密方法,可用于上述的计算机等,图4是根据本发明实施例的基于国密CEPH对象存储的加密方法的流程图,如图4所示,该流程包括如下步骤:

[0084] 步骤S401,对CEPH对象存储系统进行国产加密算法以及国产加密库的部署。详细请参见图1所示实施例的步骤S101,在此不再赘述。

[0085] 步骤S402,获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据。详细请参见图1所示实施例的步骤S102,在此不再赘述。

[0086] 步骤S403,获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,预设秘钥长度为国产加密算法对应的秘钥长度。详细请参见图1所示实施例的步骤S103,在此不再赘述。

[0087] 步骤S404,调用国产加密库并通过第二加密秘钥对文件数据进行加密。详细请参见图1所示实施例的步骤S104,在此不再赘述。

[0088] 步骤S405,获取生成的密文数据,并对密文数据进行验证。

[0089] 本发明实施例中,可以理解的是,在加密过程中,国产加密库会生成密文数据(即已经通过加密算法进行加密的文件数据)。从加密库中获取生成的密文数据,对密文数据进行验证,可以通过使用验证算法或函数,例如比较生成的哈希值或进行数字签名验证等。如果验证通过,说明密文数据没有被篡改或损坏,进入后续步骤操作。如果验证失败,则可能说明密文数据在传输或存储过程中受到了干扰或篡改,需要重新对数据进行加密。

[0090] 步骤S406,创建CEPH对象加密存储桶,将验证通过后的密文数据存储至CEPH对象加密存储桶。

[0091] 示例性的,通过执行命令或调用相应的API创建一个加密存储桶,在创建存储桶时,指定相关的参数,例如存储桶名称、访问权限等,然后通过使用CEPH提供的上传接口、命令将经过验证通过的密文数据上传或复制到所创建的加密存储桶中。

[0092] 对于本实施例,通过获取生成的密文数据并进行验证,并创建CEPH对象加密存储桶将验证通过的密文数据存储其中,实现对加密数据的集中存储,从而确保加密后的数据完整性。

[0093] 在一具体实施例中,参照图5,客户端软件将数据及相关信息上传到CEPH对象存储网关后,CEPH对象存储系统将判断信息中的秘钥长度,判断是否直接可用,如果直接可用

(即秘钥长度满足国密加密算法的要求),则直接导入预处理后的数据和信息到CEPH的加密模块,加密模块启动加密功能,判断是否配置了加密模块的外置引擎,如果是的话则GmSSL(国产加密库)将会调用内部同意引擎接口与外部加密卡实现数据对接加密;如果不是,则GmSSL(国产加密库)直接使用本地系统资源进行数据加密。完成加密后,可以进入CEPH其他处理模块,加密数据也可以保存到数据桶内。

[0094] 在本实施例中还提供了一种基于国密CEPH对象存储的加密装置,该装置用于实现上述实施例及优选实施方式,已经进行过说明的不再赘述。如以下所使用的,术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现,但是硬件,或者软件和硬件的组合的实现也是可能并被构想的。

[0095] 本实施例提供一种基于国密CEPH对象存储的加密装置,如图6所示,包括:

[0096] 配置及部署模块601,用于对CEPH对象存储系统进行国产加密算法以及国产加密库的部署;

[0097] 数据获取模块602,用于获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据;

[0098] 秘钥计算模块603,用于获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度,若不是,则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,预设秘钥长度为国产加密算法对应的秘钥长度;

[0099] 国产加密模块604,用于调用国产加密库并通过第二加密秘钥对文件数据进行加密。

[0100] 在一种可选的实施方式中,配置及部署模块601,包括:

[0101] 将CEPH对象网关的源代码中加密算法设置为国密算法;

[0102] 将CEPH对象网关的源代码中加密插件中的默认加密库设置为国产加密库;编译CEPH对象网关源代码,成功编译后对CEPH对象存储系统进行基本部署。

[0103] 在一种可选的实施方式中,配置及部署模块601,包括:

[0104] 将CEPH对象网关的源代码中默认加密库的加密函数修改为国产加密库对应的加密函数;

[0105] 将CEPH对象网关的模块中默认加密库的命名修改为国产加密库的命名。

[0106] 在一些可选的实施方式中,秘钥计算模块603,还包括:若是,则将第一加密秘钥直接设置为第二加密秘钥。

[0107] 在一些可选的实施方式中,装置还包括文件处理模块,用于:

[0108] 基于CEPH对象存储系统支持的格式对原始的文件数据进行格式处理,得到处理后的文件数据。

[0109] 在一些可选的实施方式中,国产加密模块604,包括:基于CEPH对象存储系统的配置文件获取配置信息;

[0110] 判断配置信息中指定路径下是否配置外部加密引擎,若存在,则通过国产加密库使用外部加密引擎接口调用外置加密卡对文件数据进行加密;若不存在,则调用国产加密库使用CEPH对象存储系统内置算法对文件数据进行加密。

[0111] 在一些可选的实施方式中,装置还包括数据存储模块,用于:

[0112] 获取生成的密文数据,并对密文数据进行验证;

[0113] 创建CEPH对象加密存储桶,将验证通过后的密文数据存储至CEPH对象加密存储桶。

[0114] 上述各个模块和单元的更进一步的功能描述与上述对应实施例相同,在此不再赘述。

[0115] 本发明实施例通过部署国产加密算法和加密库,确保使用的是符合国家标准的加密算法和库。获取元数据中的第一加密秘钥的长度,并判断是否与预设秘钥长度相同。如果不相同,将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥,保证秘钥为国产加密算法对应的秘钥。调用国产加密库,使用第二加密秘钥对文件数据进行加密。使用国产的加密算法和加密库,可以确保数据的加密过程符合国内的加密标准,无需适用国外的加密标准,有效保护CEPH对象存储系统中的数据,避免数据受到潜在的安全威胁,提高了数据安全性。

[0116] 本实施例中的基于国密CEPH对象存储的加密装置是以功能单元的形式来呈现,这里的单元是指ASIC(Application Specific Integrated Circuit,专用集成电路)电路,执行一个或多个软件或固定程序的处理器和存储器,和/或其他可以提供上述功能的器件。

[0117] 本发明实施例还提供一种计算机设备,具有上述图6所示的基于国密CEPH对象存储的加密装置。

[0118] 请参阅图7,图7是本发明可选实施例提供的一种计算机设备的结构示意图,如图7所示,该计算机设备包括:一个或多个处理器10、存储器20,以及用于连接各部件的接口,包括高速接口和低速接口。各个部件利用不同的总线互相通信连接,并且可以被安装在公共主板上或者根据需要以其它方式安装。处理器可以对在计算机设备内执行的指令进行处理,包括存储在存储器中或者存储器上以在外部输入/输出装置(诸如,耦合至接口的显示设备)上显示GUI的图形信息的指令。在一些可选的实施方式中,若需要,可以将多个处理器和/或多条总线与多个存储器和多个存储器一起使用。同样,可以连接多个计算机设备,各个设备提供部分必要的操作(例如,作为服务器阵列、一组刀片式服务器、或者多处理器系统)。图7中以一个处理器10为例。

[0119] 处理器10可以是中央处理器,网络处理器或其组合。其中,处理器10还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路,可编程逻辑器件或其组合。上述可编程逻辑器件可以是复杂可编程逻辑器件,现场可编程逻辑门阵列,通用阵列逻辑或其任意组合。

[0120] 其中,存储器20存储有可由至少一个处理器10执行的指令,以使至少一个处理器10执行实现上述实施例示出的方法。

[0121] 存储器20可以包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需要的应用程序;存储数据区可存储根据计算机设备的使用所创建的数据等。此外,存储器20可以包括高速随机存取存储器,还可以包括非瞬时存储器,例如至少一个磁盘存储器件、闪存器件、或其他非瞬时固态存储器件。在一些可选的实施方式中,存储器20可选包括相对于处理器10远程设置的存储器,这些远程存储器可以通过网络连接至该计算机设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0122] 存储器20可以包括易失性存储器,例如,随机存取存储器;存储器也可以包括非易

失性存储器,例如,快闪存储器,硬盘或固态硬盘;存储器20还可以包括上述种类的存储器的组合。

[0123] 该计算机设备还包括通信接口30,用于该计算机设备与其他设备或通信网络通信。

[0124] 本发明实施例还提供了一种计算机可读存储介质,上述根据本发明实施例的方法可在硬件、固件中实现,或者被实现为可记录在存储介质,或者被实现通过网络下载的原始存储在远程存储介质或非暂时机器可读存储介质中并将被存储在本地存储介质中的计算机代码,从而在此描述的方法可被存储在使用通用计算机、专用处理器或者可编程或专用硬件的存储介质上的这样的软件处理。其中,存储介质可为磁碟、光盘、只读存储记忆体、随机存储记忆体、快闪存储器、硬盘或固态硬盘等;进一步地,存储介质还可以包括上述种类的存储器的组合。可以理解,计算机、处理器、微处理器控制器或可编程硬件包括可存储或接收软件或计算机代码的存储组件,当软件或计算机代码被计算机、处理器或硬件访问且执行时,实现上述实施例示出的方法。

[0125] 虽然结合附图描述了本发明的实施例,但是本领域技术人员可以在不脱离本发明的精神和范围的情况下做出各种修改和变型,这样的修改和变型均落入由所限定的范围之内。

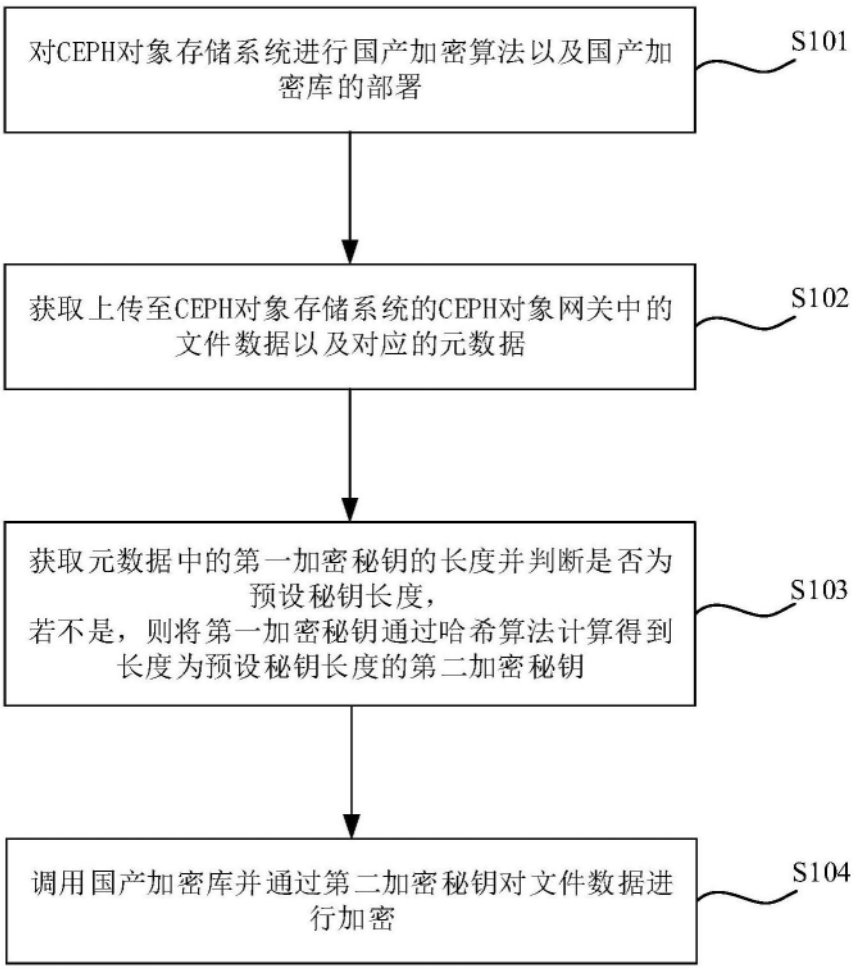

对CEPH对象存储系统进行国产加密算法以及国产加密库的部署
S101
获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据
S102
获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度，
若不是，则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥
S103
调用国产加密库并通过第二加密秘钥对文件数据进行加密
S104

图1

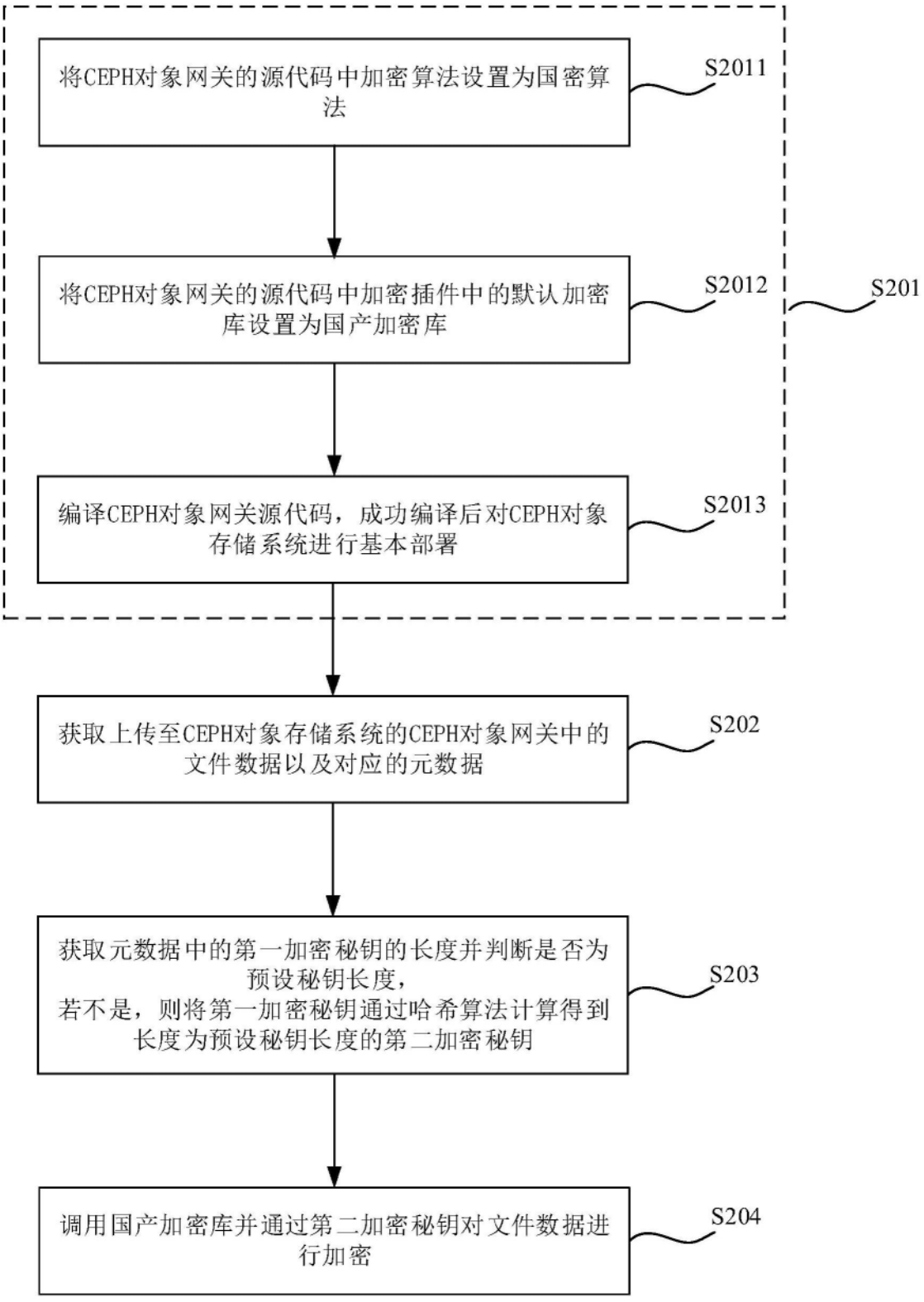

将CEPH对象网关的源代码中加密算法设置为国密算法
S2011
将CEPH对象网关的源代码中加密插件中的默认加密库设置为国产加密库
S2012
S201
编译CEPH对象网关源代码，成功编译后对CEPH对象存储系统进行基本部署
S2013
获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据
S202
获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度，
若不是，则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥
S203
调用国产加密库并通过第二加密秘钥对文件数据进行加密
S204

图2

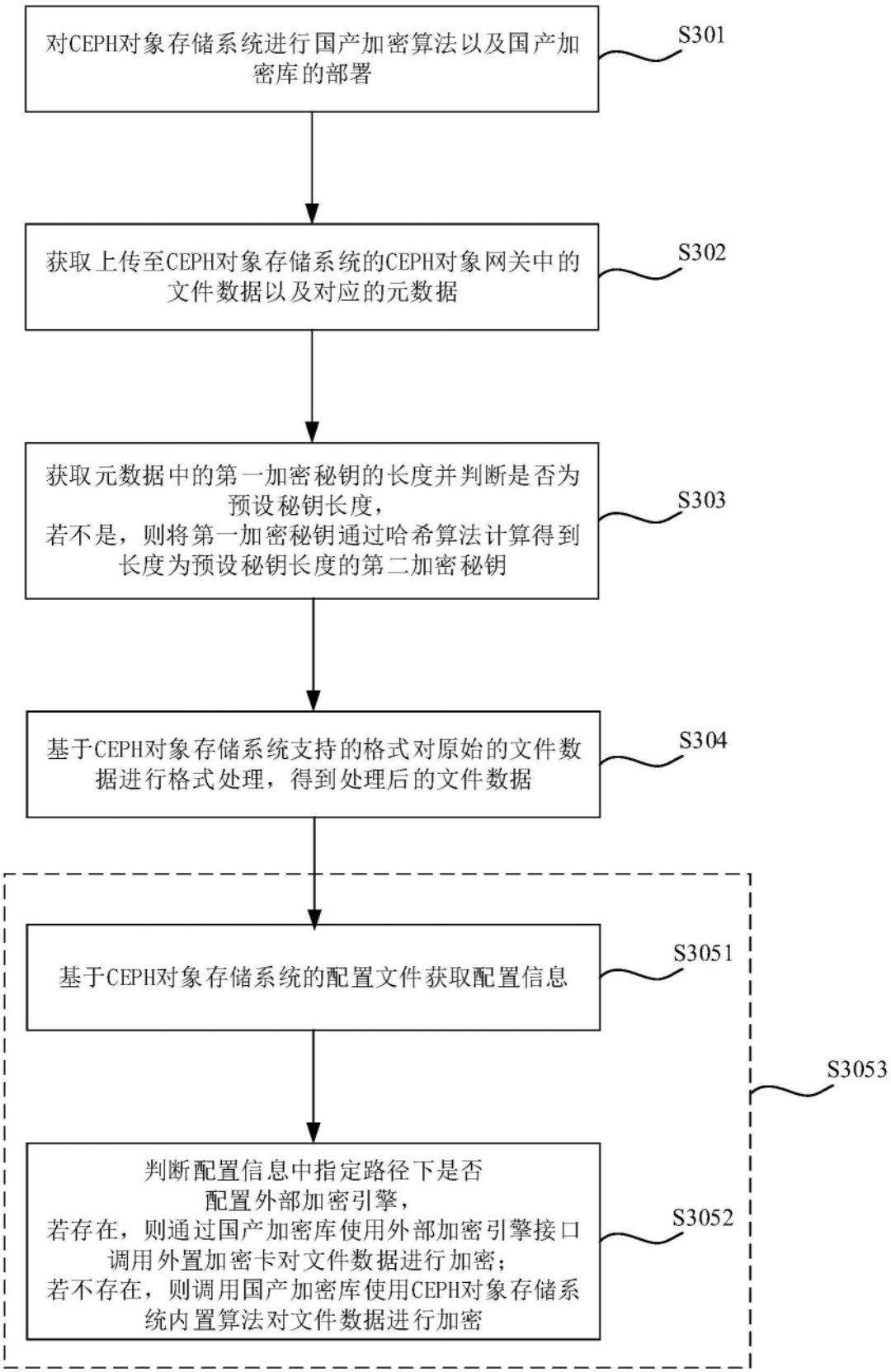

对CEPH对象存储系统进行国产加密算法以及国产加密库的部署
S301
获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据
S302
获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度，
若不是，则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥
S303
基于CEPH对象存储系统支持的格式对原始的文件数据进行格式处理，得到处理后的文件数据
S304
基于CEPH对象存储系统的配置文件获取配置信息
S3051
判断配置信息中指定路径下是否配置外部加密引擎，
若存在，则通过国产加密库使用外部加密引擎接口调用外置加密卡对文件数据进行加密；
若不存在，则调用国产加密库使用CEPH对象存储系统内置算法对文件数据进行加密
S3052
S3053

图3

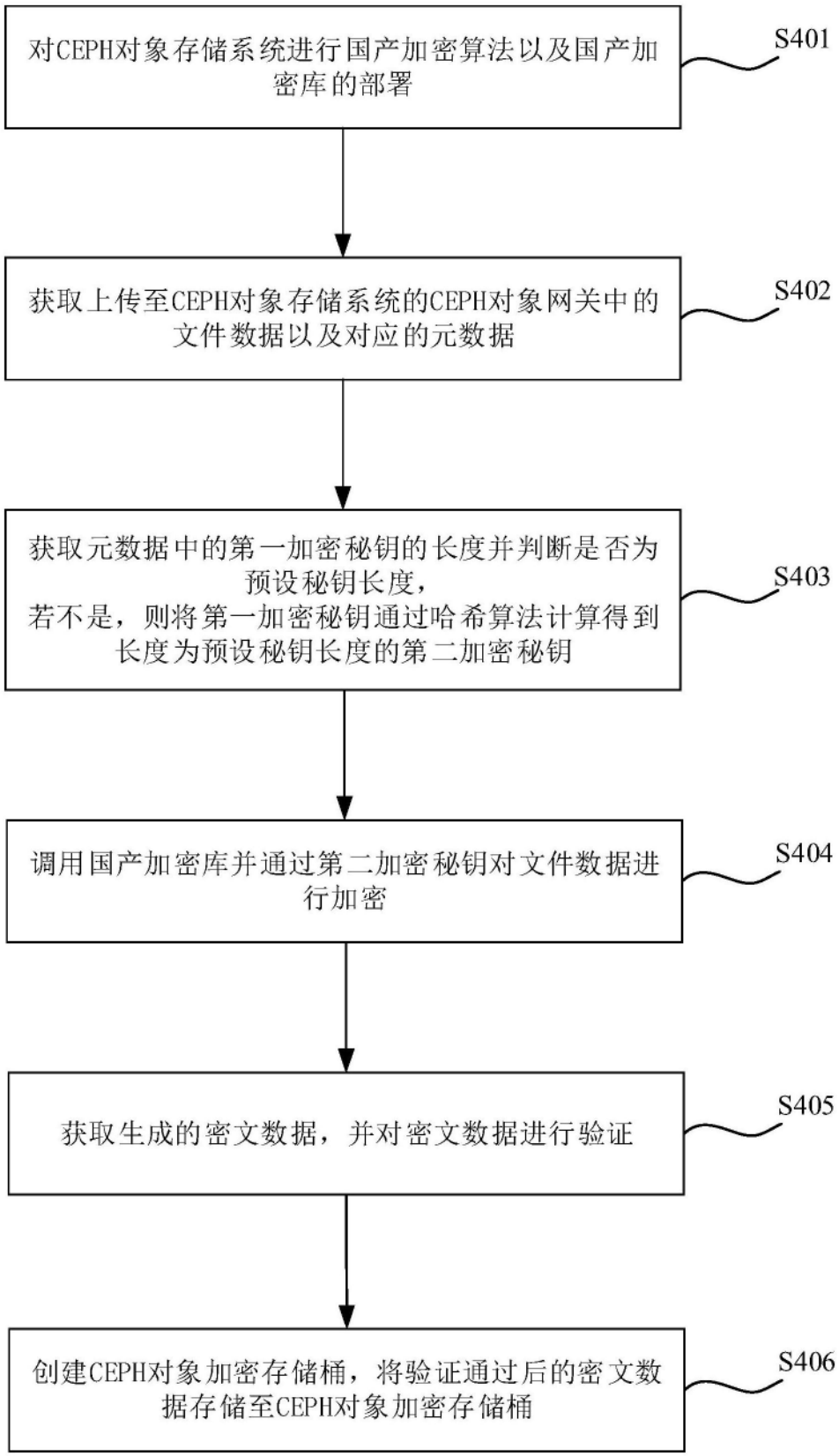

对CEPH对象存储系统进行国产加密算法以及国产加密库的部署
S401
获取上传至CEPH对象存储系统的CEPH对象网关中的文件数据以及对应的元数据
S402
获取元数据中的第一加密秘钥的长度并判断是否为预设秘钥长度，
若不是，则将第一加密秘钥通过哈希算法计算得到长度为预设秘钥长度的第二加密秘钥
S403
调用国产加密库并通过第二加密秘钥对文件数据进行加密
S404
获取生成的密文数据，并对密文数据进行验证
S405
创建CEPH对象加密存储桶，将验证通过后的密文数据存储至CEPH对象加密存储桶
S406

图4

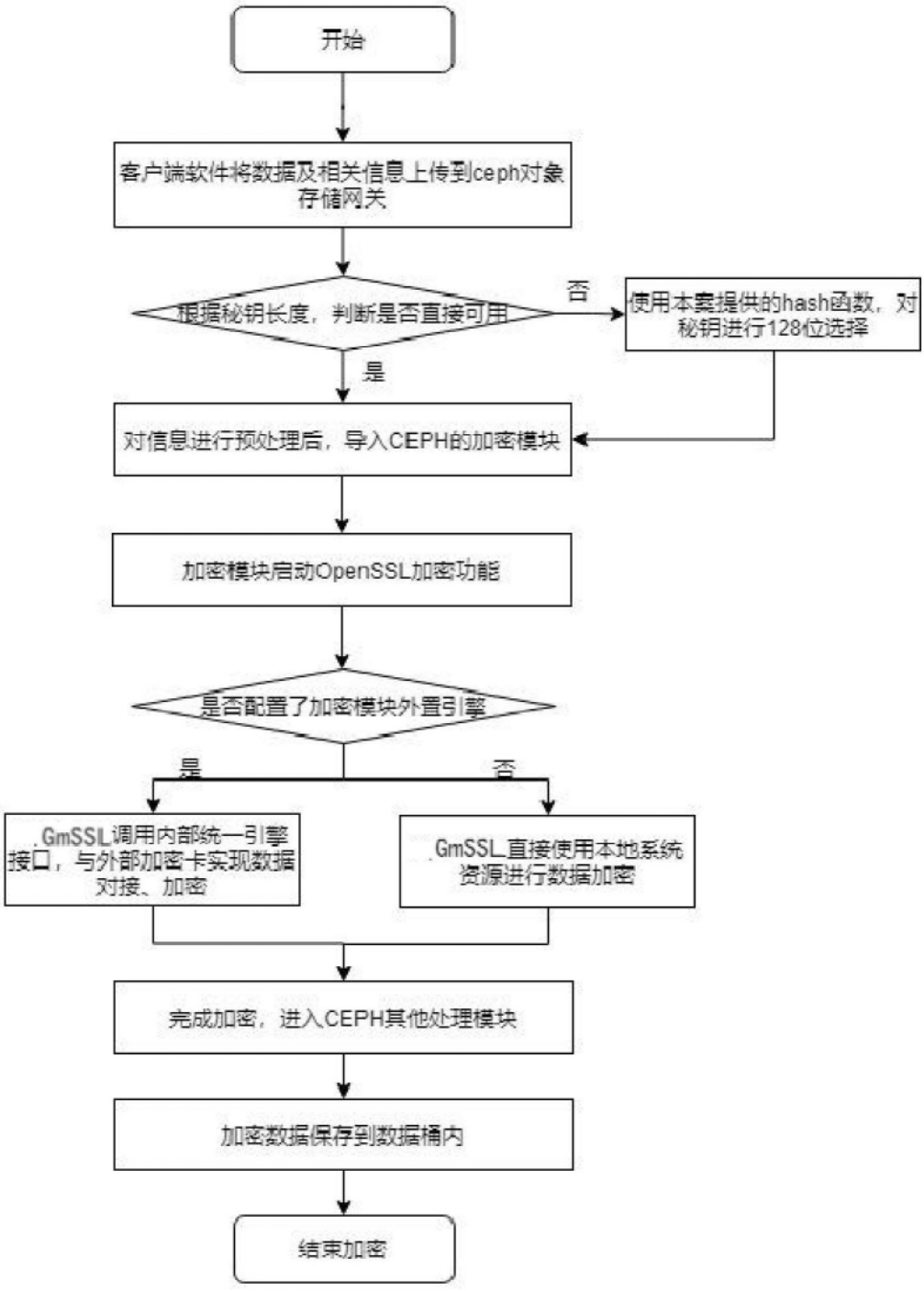

开始
客户端软件将数据及相关信息上传到ceph对象存储网关
根据秘钥长度，判断是否直接可用
否
使用本套提供的hash函数，对秘钥进行128位选择
是
对信息进行预处理后，导入CEPH的加密模块
加密模块启动OpenSSL加密功能
是否配置了加密模块外置引擎
是
否
GmSSL调用内部统一引擎接口，与外部加密卡实现数据对接、加密
GmSSL直接使用本地系统资源进行数据加密
完成加密，进入CEPH其他处理模块
加密数据保存到数据桶内
结束加密

图5

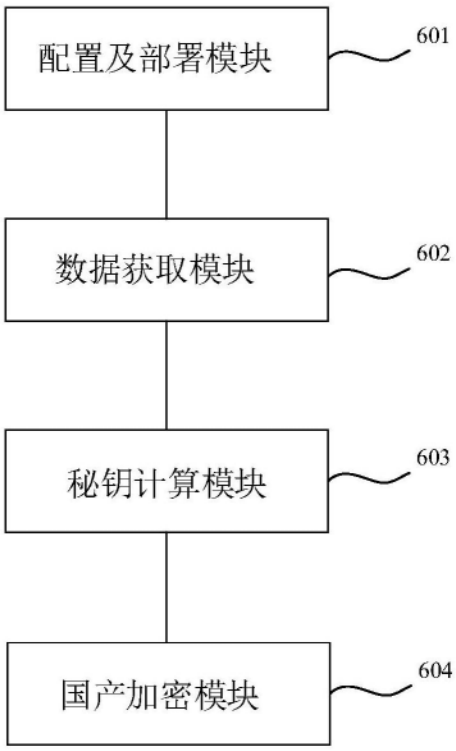

配置及部署模块
601
数据获取模块
602
秘钥计算模块
603
国产加密模块
604

图6

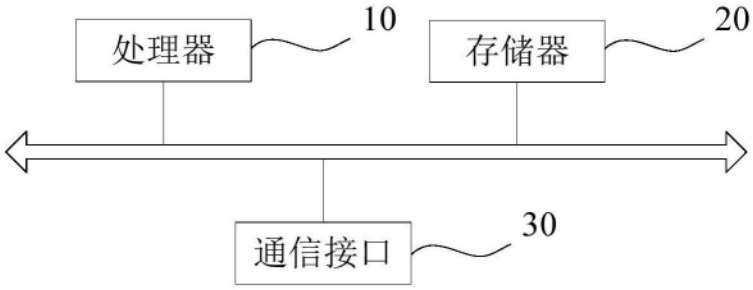

处理器
10
存储器
20
通信接口
30

图7