

(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
2017年2月9日 (09.02.2017)



(10) 国际公布号
WO 2017/020720 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2016/090821
- (22) 国际申请日: 2016年7月21日 (21.07.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510469417.7 2015年8月3日 (03.08.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 程霖 (CHENG, Lin) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。应叶琦 (YING, Yeqi) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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)。

[见续页]

(54) Title: METHOD AND DEVICE FOR DATA ACCESS

(54) 发明名称: 一种数据访问的方法及设备

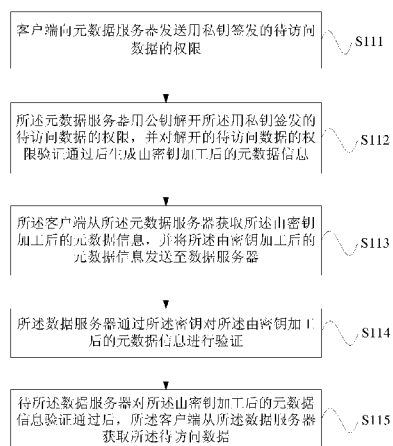


图 11

S111 A CLIENT SENDING, TO A METADATA SERVER, A PERMISSION OF DATA TO BE ACCESSED, WHICH IS SIGNED AND ISSUED USING A PRIVATE KEY
S112 THE METADATA SERVER UNLOCKING, BY USING A PUBLIC KEY, THE PERMISSION OF THE DATA TO BE ACCESSED, WHICH IS SIGNED AND ISSUED USING THE PRIVATE KEY, AND GENERATING METADATA INFORMATION PROCESSED BY A SECRET KEY AFTER THE UNLOCKED PERMISSION OF THE DATA TO BE ACCESSED PASSES THE VERIFICATION
S113 THE CLIENT ACQUIRING THE METADATA INFORMATION PROCESSED BY THE SECRET KEY FROM THE METADATA SERVER, AND SENDING SAME TO A DATA SERVER
S114 THE DATA SERVER VERIFYING, BY MEANS OF THE SECRET KEY, THE METADATA INFORMATION PROCESSED BY THE SECRET KEY
S115 THE CLIENT ACQUIRING THE DATA TO BE ACCESSED FROM THE DATA SERVER AFTER THE METADATA INFORMATION PROCESSED BY THE SECRET KEY PASSES THE VERIFICATION OF THE DATA SERVER

(57) Abstract: Provided are a method and device for data access. In the present application, a metadata server unlocks, by using a public key, a permission of the data to be accessed, which is signed and issued using a private key, and generates the metadata information processed by a secret key after the unlocked data to be accessed passes the verification, thus access control over the metadata server can be realized, so that the security of the metadata server may be ensured; in addition, only after the metadata information processed by the secret key passes the verification, the data server allows a client to acquire the data to be accessed from the data server, and this may realize an access control over the data server, so that the security of the data server may be ensured, and the anti-counterfeiting of the client may be realized finally.

(57) 摘要: 本申请提供一种数据访问的方法及设备, 本申请通过所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限, 并对解开的待访问数据的权限验证通过后, 生成所述由密钥加密后的元数据信息, 可以实现对元数据服务器的访问控制, 这样可以确保元数据服务器的安全性, 另外, 在所述数据服务器对所述由密钥加密后的元数据信息验证通过后, 才允许客户端从所述数据服务器获取所述待访问数据, 可以实现对

数据服务器的访问控制, 这样可以确保数据服务器的安全性, 最终实现客户端的防伪造性。



WO 2017/020720 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种数据访问的方法及设备

技术领域

本申请涉及计算机领域，尤其涉及一种数据访问的方法及设备。

5

背景技术

随着大数据时代的到来，为了解决分布式环境下海量数据的存储问题，怎么能够利用价格低廉的普通机器来实现海量数据的存储问题，提出了分布式文件系统 HDFS。后来这个 HDFS 系统的架构基本成为了分布式文件系统的通用框架。分布式文件系统或多或少都存在网络安全相关的威胁。尤其是在公有云中不可信用户的访问，数据必须要做到相互隔离，用户访问数据需要具备一定的访问控制权限。分布式文件系统中，元数据服务器

(NameNode)，用于存储用户文件的元数据信息。数据服务器(DataNode)，用于存储用户文件的数据信息，元数据服务器 (NameNode) 和数据服务器 (DataNode) 都会由客户端 (client) 即访问分布式文件系统的用户来访问，客户端的信息容易被篡改，因此需要做一定的访问控制策略，做到用户与数据的隔离，保证安全。

在现有的分布式文件系统中，业界没有较好的实现访问控制策略。通常使用 ACL 方式设置用户的权限，ACL 即访问控制列表，是一种基于对象的授权，这种方式是以访问的对象为出发点，但是黑客还是可以篡改数据服务器上的数据，对于元数据服务器和数据服务器之间的权限安全控制问题，目前业界并没有好的解决方案。

发明内容

本申请的一个目的是提供一种用于数据访问的方法及设备，能够解决进行数据访问时，元数据服务器和数据服务器之间的权限安全控制问题。

根据本申请的一个方面，提供了一种客户端用于数据访问的方法，该方法包括：

向元数据服务器发送用私钥签发的待访问数据的权限；

5 从元数据服务器获取由密钥加工后的元数据信息，其中，所述用私钥签发的待访问数据的权限由所述元数据服务器用公钥解开，所述由密钥加工后的元数据信息由所述元数据服务器对解开的待访问数据的权限验证通过后生成；

10 将所述由密钥加工后的元数据信息发送至数据服务器，待所述数据服务器对所述由密钥加工后的元数据信息验证通过后，从所述数据服务器获取所述待访问数据，其中，所述由密钥加工后的元数据信息由所述数据服务器通过所述密钥进行验证。

进一步的，上述方法中，向元数据服务器发送用私钥签发的待访问数据的权限的同时，还包括：

向元数据服务器发送所述待访问数据的权限的过期时间；

15 所述元数据服务器对解开的待访问数据的权限验证通过，包括：

所述元数据服务器根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，则验证通过。

进一步的，上述方法中，所述元数据服务器对解开的待访问数据的权限验证通过，包括：

20 所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。

进一步的，上述方法中，所述由密钥加工后的元数据信息包括：

元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据；

25 所述数据服务器对所述由密钥加工后的元数据信息验证通过，包括：

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密，并

将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，如果比较一致，则验证通过；

从所述数据服务器获取所述待访问数据，包括：

根据所述元数据从所述数据服务器获取所述待访问数据。

5 进一步的，上述方法中，所述由密钥加工后的元数据信息包括：

元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间；

所述数据服务器对所述由密钥加工后的元数据信息验证通过，包括：

10 所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则验证通过；

从所述数据服务器获取所述待访问数据，包括：

根据所述元数据从所述数据服务器获取所述待访问数据。

15 根据本申请的另一面还提供一种元数据服务器端用于辅助数据访问的方法，该方法包括：

从客户端接收用私钥签发的待访问数据的权限；

20 用公钥解开所述用私钥签发的待访问数据的权限，对解开的待访问数据的权限验证通过后生成由密钥加工后的元数据信息；

将所述由密钥加工后的元数据信息发送至所述客户端。

进一步的，上述方法中，从客户端接收用私钥签发的待访问数据的权限的同时，还包括：

从所述客户端接收所述待访问数据的权限的过期时间；

25 对解开的待访问数据的权限验证通过，包括：

根据所述权限的过期时间对解开的待访问数据的权限判断为未过期

时，则验证通过。

进一步的，上述方法中，对解开的待访问数据的权限验证通过，包括：

根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。

5 进一步的，上述方法中，所述由密钥加工后的元数据信息包括：

元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据。

进一步的，上述方法中，所述由密钥加工后的元数据信息还包括：

元数据的过期时间。

10

根据本申请的另一面，还提供一种数据服务器端用于辅助数据访问的方法，该方法包括：

从客户端获取由密钥加工后的元数据信息；

通过所述密钥对所述由密钥加工后的元数据信息进行验证；

15 对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据。

进一步的，上述方法中，当所述元数据信息包括元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据时，对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据，

20 包括：

用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，如果比较一致，则验证通过；

根据所述元数据向所述客户端传输所述待访问数据。

25 进一步的，上述方法中，当所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数

据及元数据的过期时间时，对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据，包括：

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则验证通过；

根据所述元数据向所述客户端传输所述待访问数据。

根据本申请的另一面还提供一种用于数据访问的客户端，该客户端包括：

发送权限装置，用于向元数据服务器发送用私钥签发的待访问数据的权限；

获取元数据装置，用于从元数据服务器获取由密钥加工后的元数据信息，其中，所述用私钥签发的待访问数据的权限由所述元数据服务器用公钥解开，所述由密钥加工后的元数据信息由所述元数据服务器对解开的待访问数据的权限验证通过后生成；

获取数据装置，用于将所述由密钥加工后的元数据信息发送至数据服务器，待所述数据服务器对所述由密钥加工后的元数据信息验证通过后，从所述数据服务器获取所述待访问数据，其中，所述由密钥加工后的元数据信息由所述数据服务器通过所述密钥进行验证。

进一步的，上述客户端中，所述客户端还包括发送过期时间装置，用于在向元数据服务器发送用私钥签发的待访问数据的权限的同时，向元数据服务器发送所述待访问数据的权限的过期时间，其中，所述元数据服务器，用于根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，则验证通过。

进一步的，上述客户端中，所述元数据服务器，用于根据预设的权限

阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。

进一步的，上述客户端中，所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据；

所述数据服务器，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，如果比较一致，则验证通过；

获取数据装置，用于根据所述元数据从所述数据服务器获取所述待访问数据。

进一步的，上述客户端中，所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间；

所述数据服务器，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则验证通过；

所述获取数据装置，用于根据所述元数据从所述数据服务器获取所述待访问数据。

根据本申请的另一面还提供一种辅助数据访问的元数据服务器，该元数据服务器包括：

接收权限装置，用于从客户端接收用私钥签发的待访问数据的权限；

生成元数据装置，用于用公钥解开所述用私钥签发的待访问数据的权限，对解开的待访问数据的权限验证通过后生成由密钥加工后的元数据信息；

发送元数据装置，用于将所述由密钥加工后的元数据信息发送至所述客户端。

进一步的，上述元数据服务器中，所述元数据服务器还包括接收过期时间装置，用于从所述客户端接收所述待访问数据的权限的过期时间；

5 所述生成元数据装置，用于根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，则验证通过。

进一步的，上述元数据服务器中，所述生成元数据装置，用于根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。

10 进一步的，上述元数据服务器中，所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据。

进一步的，上述元数据服务器中，所述由密钥加工后的元数据信息还包括：元数据的过期时间。

15

根据本申请的另一面还提供一种辅助数据访问的数据服务器，其中，该数据服务器包括：

元数据装置，用于从客户端获取由密钥加工后的元数据信息；

20 验证装置，用于通过所述密钥对所述由密钥加工后的元数据信息进行验证；

数据传输装置，用于对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据。

进一步的，上述数据服务器中，当所述元数据信息包括元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据时，所述
25 数据传输装置，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行

比较, 如果比较一致, 则验证通过; 根据所述元数据向所述客户端传输所述待访问数据。

进一步的, 上述数据服务器中, 当所述由密钥加工后的元数据信息包括: 元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间时, 所述数据传输装置, 用于用所述密钥对接收到的所述部分元数据进行本地加密, 并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较, 并根据所述元数据的过期时间判断元数据是否过期, 如果比较一致且元数据未过期, 则验证通过; 根据所述元数据向所述客户端传输所述待访问数据。

与现有技术相比, 本申请通过所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限, 并对解开的待访问数据的权限验证通过后, 生成所述由密钥加工后的元数据信息, 可以实现对元数据服务器的访问控制, 这样可以确保元数据服务器的安全性, 另外, 在所述数据服务器对所述由密钥加工后的元数据信息验证通过后, 才允许客户端从所述数据服务器获取所述待访问数据, 可以实现对数据服务器的访问控制, 这样可以确保数据服务器的安全性, 最终实现客户端的抗伪造性。

进一步的, 本申请在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后, 进一步增加附加的条件, 即所述元数据服务器根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时, 当同时满足此附加的条件的时候, 才判断为对解开的待访问数据的权限验证通过, 进而更严格地对待访问数据的权限进行验证, 对不满足附加条件的情况, 则不允许客户端后续对数据服务器的访问, 保证后续需要访问的数据服务器上的数据安全性。

进一步的, 本申请在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后, 进一步增加附加的条件, 即所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时, 则

判断为满足附加的条件，当解开的待访问数据的权限过大，超过所述预设的权限阈值，则判断为不满足附加的条件，当同时满足附加的条件的时候，才判断为对解开的待访问数据的权限验证通过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不允许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全性。

进一步的，本申请中所述数据服务器用所述密钥对接收到的所述部分无数进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，在如果比较一致，才验证通过，因为客户端没有密钥（key），说明客户端是可信的，这样，客户端就可以与数据服务器建立可信连接，就可以安全地传输待访问数据。

进一步的，本申请中所述数据服务器用所述密钥对接收到的所述部分无数进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，满足比较一致的条件同时，还需要另一条件，即数据服务器判断元数据未过期，两个条件都满足后，才判断为验证通过，可以进行后续对数据服务器的访问，从而实现对所述由密钥加工后的元数据信息验证更严格的验证，保证客户端的可信度。

附图说明

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：

图 1 示出根据本申请一个方面的一种客户端用于数据访问的方法的流程图；

图 2 示出本申请一个实施例的分布式文件系统架构图；

图 3 示出根据本申请一个实施例的客户端会向元数据服务器发送的信息内容示意图；

图 4 示出根据本申请另一个方面的元数据服务器端用于辅助数据访问的方法的流程图；

图 5 示出根据本申请另一个方面的数据服务器端用于辅助数据访问的方法的流程图；

5 图 6 示出根据本申请另一个方面的用于数据访问的客户端的模块图；

图 7 示出根据本申请一个优选实施例的用于数据访问的客户端的模块图；

图 8 示出根据本申请另一个方面的辅助数据访问的元数据服务器的模块图；

10 图 9 示出根据本申请一个优选实施例的辅助数据访问的元数据服务器的模块图；

图 10 示出根据本申请另一个方面的辅助数据访问的数据服务器的模块图；

图 11 示出根据本申请一个具体应用实施例的流程图。

15 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

下面结合附图对本发明作进一步详细描述。

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
20 一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

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。

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
25 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。

如图 1 所示, 本申请提供一种客户端用于数据访问的方法, 其中, 该方法包括:

步骤 S11, 向元数据服务器发送用私钥签发的待访问数据的权限; 具体的, 如图 2 所示, 分布式文件系统架构由三方来参与: Client 端(客户端 1)、NameNode 端(元数据服务器 2)、DataNode 端(数据服务器 3), 其中, 图中 HA(High Available)为高可用性集群, 是保证业务连续性的有效解决方案, 一般有两个或两个以上的节点, 且分为活动节点及备用节点, 这三方的通信可以是基于 RPC 协议来通信, 建立在 TCP/IP 协议之上, 元数据服务器存储着待访问数据的元数据信息 (meta), 元数据信息用于记录待访问数据在数据服务器上存储位置的信息, 客户端通过从元数据服务器获取元数据信息, 然后通过元数据信息直接访问数据服务器获取所需要的待访问数据, 对于元数据服务器的访问控制可以使用能力鉴权 (Capability) 的方式, Capability 是用于访问控制的一种数据结构, 其定义了对一个或多个指定的资源(如目录、文件等)所具有的访问权限, 能力鉴权需要包括私钥 (Signature) 和待访问数据的权限(Permissions), 以便客户端向元数据服务器发送用私钥签发的待访问数据的权限, 在此待访问数据的权限(Permissions)可以是一个权限集合列表, 每一个 permission 可以有两个字段: 权限集合编号 resourceID 和对应于权限集合编号的权限集合 (permission bundle), 可以根据需要设置权限

集合的数据位数，如可设置 32bits，每个 bit 表示用户定义的一个权限，待访问数据的权限可以包括：READ（读权限）、WRITE(写权限)、ROOT(读写权限，等价于 READ|WRITE)；

步骤 S12，从元数据服务器获取由密钥加工后的元数据信息，其中，

5 所述用私钥签发的待访问数据的权限由所述元数据服务器用公钥解开，所述由密钥加工后的元数据信息由所述元数据服务器对解开的待访问数据的权限验证通过后生成；在此，所述公钥是对应于所述私钥的公钥，以方便所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限，当客户端去访问元数据服务器的时候，向元数据服务器发送用私钥签发的待

10 访问数据的权限，然后元数据服务器拿到该用私钥签发的待访问数据的权限之后需要作验证，如果验证通过，客户端就可以从元数据服务器获取由密钥加工后的元数据信息，进而继续后续对数据服务器的访问，例如，当客户端 client1 请求读取待访问数据 file1 的内容，RPC 协议下请求格式为：(/client1/file1, READ),客户端会向元数据服务器发送该请求的用私钥签发的

15 的待访问数据的权限，这个时候客户端会向元数据服务器发送的消息内容具体可参见图 3，消息内容包括：消息头（A）、包含具体请求内容的消息体（B）及用私钥签发的待访问数据的权限（C），客户端可用 protocolbuffer（google 的一种数据交换的格式）格式来传输消息内容,然后元数据服务器拿到用私钥签发的待访问数据的权限之后，利用公钥解开用私钥签发的

20 待访问数据的权限，然后对解开的待访问数据的权限验证通过后生成所述由密钥加工后的元数据信息，客户端从元数据服务器获取由密钥加工后的元数据信息，其中，所述用私钥签发的待访问数据的权限可由客户端自己生成，也可由另外的第三方生成后，由客户端从所述第三方获取，另外，当客户端能够利用公钥解开用私钥签发的待访问数据的权限，即可判断为对

25 解开的待访问数据的权限验证通过，也可以在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后，进一步增加附加的条件，当同时

满足附加的条件的时候，才判断为对解开的待访问数据的权限验证通过；

步骤 S13，将所述由密钥加工后的元数据信息发送至数据服务器，待所述数据服务器对所述由密钥加工后的元数据信息验证通过后，从所述数据服务器获取所述待访问数据，其中，所述由密钥加工后的元数据信息由所述数据服务器通过所述密钥进行验证。本实施例通过所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限，并对解开的待访问数据的权限验证通过后，生成所述由密钥加工后的元数据信息，可以实现对元数据服务器的访问控制，这样可以确保元数据服务器的安全性，另外，在所述数据服务器对所述由密钥加工后的元数据信息验证通过后，才允许客户端从所述数据服务器获取所述待访问数据，可以实现对数据服务器的访问控制，这样可以确保数据服务器的安全性，最终实现客户端的抗伪造性。

本申请的客户端用于数据访问的方法一优选的实施例中，步骤 S11，向元数据服务器发送用私钥签发的待访问数据的权限的同时，还包括：

向元数据服务器发送所述待访问数据的权限的过期时间(Expire)；

所述元数据服务器对解开的待访问数据的权限验证通过，包括：

所述元数据服务器根据所述权限的过期时间(Expire)对解开的待访问数据的权限判断为未过期时，则验证通过。在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后，在此进一步增加附加的条件，即所述元数据服务器根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，当同时满足此附加的条件的时候，才判断为对解开的待访问数据的权限验证通过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不允许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全性。详细的，在分布式文件系统中，能力鉴权（Capability）可定义为如下格式：

Length	Signature	ID	Expire	Permissions
--------	-----------	----	--------	-------------

其中：Length 表示 Signarure 的长度；

Signature 表示私钥，用于验证 Permissions 是否被篡改；

ID 表示 Capability 的 ID 号，是唯一的；

Expire 表示该 Capability 的过期时间；

5 Permissions 表示待访问数据的权限。

本申请的客户端用于数据访问的方法一优选的实施例中，所述元数据服务器对解开的待访问数据的权限验证通过，包括：

所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。在元数据服务器能够利用公
10 钥解开用私钥签发的待访问数据的权限后，在此进一步增加附加的条件，即所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则判断为满足附加的条件，当解开的待访问数据的权限过大，超过所述预设的权限阈值，则判断为不满足附加的条件，当同时满足附加的条件的时候，才判断为对解开的待访问数据的权限验证
15 通过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不允许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全性。

本申请的客户端用于数据访问的方法一优选的实施例中，所述由密钥加工后的元数据信息包括：

20 元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据；在此，可以在元数据服务器和数据服务器部署相同的密钥(key)，例如，可以在元数据服务器和数据服务器部署一个同样的文件(key.txt)，该文件里保存着密钥(key)，该密钥(key)必须要保存在一个安全的目录，需要特定权限才可以打开，以防止密钥被窃取，密钥(key)的长度
25 可以随机选取，长度不能太短也不能太长，可设定key的长度为16字节(128位)，密钥(key)可以使用linux操作系统的uuid生成，可以通过

/proc/sys/kernel/random/uuid 来随机生成一个 uuid 码,也可以使用 openssl 命令来生成一个密钥 key,另外,客户端请求访问元数据服务器并通过对解开的待访问数据的权限的验证的时候,元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')\msg'\msg, msg 为元数据,其中, msg'为从
5 所述元数据 (msg) 中提取的部分元数据, HMAC(key, msg')为用所述密钥 (key) 并采用 HMAC 算法加密后的部分元数据 (msg'),元数据可对由密钥加工后的元数据信息进行 protocolbuffer 序列化之后将其发送给客户端,后续客户再将序列化之后的由密钥加工后的元数据信息发送至数据服务器,在此,生成所述用所述密钥加密后的部分元数据的加密算法不限于上述
10 HMAC 算法,其中, HMAC 为消息认证码,其通过捆绑一个共享密钥可以使用任何迭代的可用于加密的散列函数;

所述数据服务器对所述由密钥加工后的元数据信息验证通过,包括:

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密,并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行
15 比较,如果比较一致,则验证通过;在此,数据服务器收到客户端发来的序列化之后的由密钥加工后的元数据信息,针对接收到的序列化后的信息进行反序列化之后,从本地部署的文件 (key.txt) 中获取密钥 (key),利用该 key 值对接收到的 msg'字段进行 HMAC (Hash-based Message Authentication Code) 算法得到 HMAC(key, msg'),看得到的 HMAC(key, msg')和接收到的
20 HMAC(key, msg')是否一样,如果一样就可以确定接收到的由密钥加工后的元数据信息是从元数据服务器获取到的,因为客户端没有密钥 (key),说明客户端是可信的,这样,客户端就可以与数据服务器建立可信连接,就可以安全地传输待访问数据了;

步骤 S13 中的从所述数据服务器获取所述待访问数据,包括:

25 根据所述元数据从所述数据服务器获取所述待访问数据。

本申请的客户端用于数据访问的方法一优选的实施例中,所述由密钥

加工后的元数据信息包括：

元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间；在此，以上述元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')\msg'\msg 为例，可以在用所述密钥加密后的部分元数据（msg'）中设置元数据的过期时间（expire_time），如 msg'={FileID, READ / WRITE, expire_time}；

所述数据服务器对所述由密钥加工后的元数据信息验证通过，包括：

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则验证通过；在此，在将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，满足比较一致的条件同时，还需要另一条件，即数据服务器判断元数据未过期，两个条件都满足后，才判断为验证通过，可以进行后续对数据服务器的访问，从而实现对所述由密钥加工后的元数据信息验证更严格的验证，保证客户端的可信度，详细的，元数据服务器通过设置客户端访问数据服务器的过期时间（expire_time），一旦这个 expire_time 到期之后，数据服务器可以触发一个到期（token expire）事件，该到期事件会发个请求给客户端，客户端需要重新向元数据服务器请求由密钥加工后的元数据信息；

步骤 S13 中的从所述数据服务器获取所述待访问数据，包括：

根据所述元数据从所述数据服务器获取所述待访问数据。

如图 4 所示，根据本申请的另一面还提供一种元数据服务器端用于辅助数据访问的方法，该方法包括：

步骤 S21，从客户端接收用私钥签发的待访问数据的权限；具体的，如图 2 所示，分布式文件系统架构由三方来参与的：Client 端（客户端 1）、NameNode 端（元数据服务器 2）、DataNode 端（数据服务器 3），这三方的通信

可以是基于 RPC 协议来通信，建立在 TCP/IP 协议之上，元数据服务器存储着待访问数据的元数据信息 (meta)，元数据信息用于记录待访问数据在数据服务器上存储位置的信息，客户端通过从元数据服务器获取元数据信息，然后通过元数据信息直接访问数据服务器获取所需要的待访问数据，对于元数据服务器的访问控制可以使用能力鉴权 (Capability) 的方式，Capability 是用于访问控制的一种数据结构，其定义了对一个或多个指定的资源(如目录、文件等)所具有的访问权限，能力鉴权需要包括私钥 (Signature) 和待访问数据的权限(Permissions)，以便客户端向元数据服务器发送用私钥签发的待访问数据的权限，在此待访问数据的权限(Permissions)可以是一个权限集合列表，每一个 permission 可以有两个字段：权限集合编号 resourceID 和对应于权限集合编号的权限集合 (permission bundle)，可以根据需要设置权限集合的数据位数，如可设置 32bits，每个 bit 表示用户定义的一个权限，待访问数据的权限可以包括：READ (读权限)、WRITE(写权限)、ROOT(读写权限，等价于 READ|WRITE)；

步骤 S22，用公钥解开所述用私钥签发的待访问数据的权限，对解开的待访问数据的权限验证通过后生成由密钥加工后的元数据信息；在此，所述公钥是对应于所述私钥的公钥，以方便所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限，当客户端去访问元数据服务器的时候，向元数据服务器发送用私钥签发的待访问数据的权限，然后元数据服务器拿到该用私钥签发的待访问数据的权限之后需要作验证，如果验证通过，客户端就可以从元数据服务器获取由密钥加工后的元数据信息，进而继续后续对数据服务器的访问，例如，当客户端 client1 请求读取待访问数据 file1 的内容，RPC 协议下请求格式为：(/client1/file1, READ),客户端会向元数据服务器发送该请求的用私钥签发的待访问数据的权限，这个时候客户端会向元数据服务器发送的消息内容具体可参见图 3，消息内容包括：消息头 (A)、包含具体请求内容的消息体 (B) 及用私钥签发的待访问数

据的权限 (C), 客户端可用 protocolbuffer (google 的一种数据交换的格式) 格式来传输消息内容, 然后元数据服务器拿到用私钥签发的待访问数据的权限之后, 利用公钥解开用私钥签发的待访问数据的权限, 然后对解开的待访问数据的权限验证通过后生成所述由密钥加工后的元数据信息, 客户端从元数据服务器获取由密钥加工后的元数据信息, 其中, 所述用私钥签发的待访问数据的权限可由客户端自己生成, 也可由另外的第三方生成后, 由客户端从所述第三方获取, 另外, 当客户端能够利用公钥解开用私钥签发的待访问数据的权限, 即可判断为对解开的待访问数据的权限验证通过, 也可以在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后, 进一步增加附加的条件, 当同时满足附加的条件的时候, 才判断为对解开的待访问数据的权限验证通过;

步骤 S23, 将所述由密钥加工后的元数据信息发送至所述客户端。本实施例通过所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限, 并对解开的待访问数据的权限验证通过后, 生成所述由密钥加工后的元数据信息, 可以实现对元数据服务器的访问控制, 这样可以确保元数据服务器的安全性。

本申请的元数据服务器端用于辅助数据访问的方法一优选的实施例中, 从客户端接收用私钥签发的待访问数据的权限的同时, 还包括:

从所述客户端接收所述待访问数据的权限的过期时间(Expire);

步骤 S22 中的对解开的待访问数据的权限验证通过, 包括:

根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时, 则验证通过。在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后, 在此进一步增加附加的条件, 即所述元数据服务器根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时, 当同时满足此附加的条件的时候, 才判断为对解开的待访问数据的权限验证通过, 进而更严格地对待访问数据的权限进行验证, 对不满足附加条件的情况,

则不充许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全性。详细的，在分布式文件系统中，能力鉴权（Capability）可定义为如下格式：

Length	Signature	ID	Expire	Permissions
--------	-----------	----	--------	-------------

其中：Length 表示 Signarure 的长度；

Signature 表示私钥，用于验证 Permissions 是否被篡改；

ID 表示 Capability 的 ID 号，是唯一的；

Expire 表示该 Capability 的过期时间；

Permissions 表示待访问数据的权限。

本申请的元数据服务器端用于辅助数据访问的方法一优选的实施例中，步骤 S22 中的对解开的待访问数据的权限验证通过，包括：

根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后，在此进一步增加附加的条件，即所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则判断为满足附加的条件，当解开的待访问数据的权限过大，超过所述预设的权限阈值，则判断为不满足附加的条件，当同时满足附加的条件的时候，才判断为对解开的待访问数据的权限验证通过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不充许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全性。

本申请的元数据服务器端用于辅助数据访问的方法一优选的实施例中，所述由密钥加工后的元数据信息包括：

元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据。在此，可以在元数据服务器和数据服务器部署相同的密钥(key)，

例如，可以在元数据服务器和数据服务器部署一个同样的文件（key.txt），该文件里保存着密钥（key），该密钥（key）必须要保存在一个安全的目录，需要特定权限才可以打开，以防止密钥被窃取，密钥（key）的长度可以随机选取，长度不能太短也不能太长，可设定key的长度为16字节(128 5 位)，密钥（key）可以使用 linux 操作系统的 uuid 生成，可以通过 /proc/sys/kernel/random/uuid 来随机生成一个 uuid 码，也可以使用 openssl 命令来生成一个密钥 key，另外，客户端请求访问元数据服务器并通过对解开的待访问数据的权限的验证的时候，元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')lmsg'lmsg, msg 为元数据，其中，msg'为从 10 所述元数据（msg）中提取的部分元数据，HMAC(key, msg')为用所述密钥（key）并采用 HMAC 算法加密后的部分元数据（msg'），元数据可对由密钥加工后的元数据信息进行 protocolbuffer 序列化之后将其发送给客户端，后续客户再将序列化之后的由密钥加工后的元数据信息发送至数据服务器，在此，生成所述用所述密钥加密后的部分元数据的加密算法不限于上述 15 HMAC 算法，其中，HMAC 为消息认证码,其通过捆绑一个共享密钥可以使用任何迭代的可用于加密的散列函数。

本申请的元数据服务器端用于辅助数据访问的方法一优选的实施例中，所述由密钥加工后的元数据信息还包括：

元数据的过期时间。在此，以上述元数据服务器返回给客户端的元数据 20 信息包括 HMAC(key, msg')lmsg'lmsg 为例，可以在用所述密钥加密后的部分元数据(msg')中设置元数据的过期时间(expire_time)，如 msg'={FileID, READ / WRITE, expire_time}。

如图 5 所示，根据本申请的另一面还提供一种数据服务器端用于辅助数据访问的方法，该方法包括：

25 步骤 S31，从客户端获取由密钥加工后的元数据信息；

步骤 S32，通过所述密钥对所述由密钥加工后的元数据信息进行验证；

步骤 S33, 对所述由密钥加工后的元数据信息验证通过后, 向所述客户端传输所述待访问数据。本实施例在所述数据服务器对所述由密钥加工后的元数据信息验证通过后, 才允许客户端从所述数据服务器获取所述待访问数据, 可以实现对数据服务器的访问控制, 这样可以确保数据服务器的安全性, 最终实现客户端的抗伪造性。

本申请的数据服务器端用于辅助数据访问的方法的一优选的实施例中, 当所述元数据信息包括元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据时, 步骤 S33, 对所述由密钥加工后的元数据信息验证通过后, 向所述客户端传输所述待访问数据, 包括:

用所述密钥对接收到的所述部分元数据进行本地加密, 并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较, 如果比较一致, 则验证通过; 在此, 可以在元数据服务器和数据服务器部署相同的密钥 (key), 例如, 可以在元数据服务器和数据服务器部署一个同样的文件 (key.txt), 该文件里保存着密钥 (key), 该密钥 (key) 必须要保存在一个安全的目录, 需要特定权限才可以打开, 以防止密钥被窃取, 密钥 (key) 的长度可以随机选取, 长度不能太短也不能太长, 可设定 key 的长度为 16 字节(128 位), 密钥 (key) 可以使用 linux 操作系统的 uuid 生成, 可以通过 /proc/sys/kernel/random/uuid 来随机生成一个 uuid 码, 也可以使用 openssl 命令来生成一个密钥 key, 另外, 客户端请求访问元数据服务器并通过对解开的待访问数据的权限的验证的时候, 元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')||msg'||msg, msg 为元数据, 其中, msg' 为从所述元数据 (msg) 中提取的部分元数据, HMAC(key, msg') 为用所述密钥 (key) 并采用 HMAC 算法加密后的部分元数据 (msg'), 元数据可对由密钥加工后的元数据信息进行 protocolbuffer 序列化之后将其发送给客户端, 后续客户再将序列化之后的由密钥加工后的元数据信息发送至数据服务器, 在此, 生成所述用所述密钥加密后的部分元数据的加密算法不限

于上述 HMAC 算法，其中，HMAC 为消息认证码，其通过捆绑一个共享密钥可以使用任何迭代的可用于加密的散列函数，数据服务器收到客户端发来的序列化之后的由密钥加工后的元数据信息，针对接收到的序列化后的信息进行反序列化之后，从本地部署的文件（key.txt）中获取密钥（key），利用该
5 key 值对接收的 msg' 字段进行 HMAC（Hash-based Message Authentication Code）算法得到 HMAC(key, msg')，看得到的 HMAC(key, msg') 和接收到的 HMAC(key, msg') 是否一样，如果一样就可以确定接收到的由密钥加工后的元数据信息是从元数据服务器获取到的，因为客户端没有密钥（key），说明客户端是可信的，这样，客户端就可以与数据服务器建立可信连接，就可以
10 安全地传输待访问数据了；

根据所述元数据向所述客户端传输所述待访问数据。

本申请的数据服务器端用于辅助数据访问的方法的一优选的实施例中，当所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间
15 时，步骤 S33，对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据，包括：

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致
20 且元数据未过期，则验证通过；在此，以上述元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')|msg'|msg 为例，可以在用所述密钥加密后的部分元数据（msg'）中设置元数据的过期时间（expire_time），如 msg'={FileID, READ / WRITE, expire_time}，在将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，满足比较一致的条件
25 同时，还需要另一条件，即数据服务器判断元数据未过期，两个条件都满足后，才判断为验证通过，可以进行后续对数据服务器的访问，从而实现

对所述由密钥加工后的元数据信息验证更严格的验证，保证客户端的可信度，详细的，元数据服务器通过设置客户端访问数据服务器的过期时间（expire_time），一旦这个 expire_time 到期之后，数据服务器可以触发一个到期（token expire）事件，该到期事件会发个请求给客户端，客户端需要重新向元数据服务器请求由密钥加工后的元数据信息；

根据所述元数据向所述客户端传输所述待访问数据。

如图 6 所示，一种用于数据访问的客户端，该客户端 1 包括：

发送权限装置 11，用于向元数据服务器 2 发送用私钥签发的待访问数据的权限；具体的，如图 2 所示，分布式文件系统架构由三方来参与：Client 端（客户端 1）、NameNode 端（元数据服务器 2）、DataNode 端（数据服务器 3），这三方的通信可以是基于 RPC 协议来通信，建立在 TCP/IP 协议之上，元数据服务器存储着待访问数据的元数据信息（meta），元数据信息用于记录待访问数据在数据服务器上存储位置的信息，客户端通过从元数据服务器获取元数据信息，然后通过元数据信息直接访问数据服务器获取所需要的待访问数据，对于元数据服务器的访问控制可以使用能力鉴权（Capability）的方式，Capability 是用于访问控制的一种数据结构，其定义了对一个或多个指定的资源（如目录、文件等）所具有的访问权限，能力鉴权需要包括私钥（Signature）和待访问数据的权限（Permissions），以便客户端向元数据服务器发送用私钥签发的待访问数据的权限，在此待访问数据的权限（Permissions）可以是一个权限集合列表，每一个 permission 可以有两个字段：权限集合编号 resourceID 和对应于权限集合编号的权限集合（permission bundle），可以根据需要设置权限集合的数据位数，如可设置 32bits，每个 bit 表示用户定义的一个权限，待访问数据的权限可以包括：READ（读权限）、WRITE（写权限）、ROOT（读写权限，等价于 READ|WRITE）；

获取元数据装置 12，用于从元数据服务器 2 获取由密钥加工后的元数据信息，其中，所述用私钥签发的待访问数据的权限由所述元数据服务器

2 用公钥解开，所述由密钥加工后的元数据信息由所述元数据服务器 2 对解开的待访问数据的权限验证通过后生成；在此，所述公钥是对应于所述私钥的公钥，以方便所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限，当客户端去访问元数据服务器的时候，向元数据服务器发送用私钥签发的待访问数据的权限，然后元数据服务器拿到该用私钥签发的待访问数据的权限之后需要作验证，如果验证通过，客户端就可以从元数据服务器获取由密钥加工后的元数据信息，进而继续后续对数据服务器的访问，例如，当客户端 client1 请求读取待访问数据 file1 的内容，RPC 协议下请求格式为：(/client1/file1, READ), 客户端会向元数据服务器发送该请求的用私钥签发的待访问数据的权限，这个时候客户端会向元数据服务器发送的消息内容具体可参见图 3，消息内容包括：消息头（A）、包含具体请求内容的消息体（B）及用私钥签发的待访问数据的权限（C），客户端可用 protocolbuffer（google 的一种数据交换的格式）格式来传输消息内容，然后元数据服务器拿到用私钥签发的待访问数据的权限之后，利用公钥解开用私钥签发的待访问数据的权限，然后对解开的待访问数据的权限验证通过后生成所述由密钥加工后的元数据信息，客户端从元数据服务器获取由密钥加工后的元数据信息，其中，所述用私钥签发的待访问数据的权限可由客户端自己生成，也可由另外的第三方生成后，由客户端从所述第三方获取，另外，当客户端能够利用公钥解开用私钥签发的待访问数据的权限，即可判断为对解开的待访问数据的权限验证通过，也可以在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后，进一步增加附加的条件，当同时满足附加的条件的时候，才判断为对解开的待访问数据的权限验证通过；

获取数据装置 13，用于将所述由密钥加工后的元数据信息发送至数据服务器 3，待所述数据服务器 3 对所述由密钥加工后的元数据信息验证通过后，从所述数据服务器 3 获取所述待访问数据，其中，所述由密钥加工后的元

数据信息由所述数据服务器通过所述密钥进行验证。本实施例通过所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限，并对解开的待访问数据的权限验证通过后，生成所述由密钥加工后的元数据信息，可以实现对元数据服务器的访问控制，这样可以确保元数据服务器的安全性，

5 另外，在所述数据服务器对所述由密钥加工后的元数据信息验证通过后，才允许客户端从所述数据服务器获取所述待访问数据，可以实现对数据服务器的访问控制，这样可以确保数据服务器的安全性，最终实现客户端的抗伪造性。

如图 7 所示，本申请用于数据访问的客户端一优选的实施例中，所述

10 客户端 1 还包括发送过期时间装置 14，用于在向元数据服务器 2 发送用私钥签发的待访问数据的权限的同时，向元数据服务器 2 发送所述待访问数据的权限的过期时间(Expire)，其中，所述元数据服务器 2，用于根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，则验证通过。在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限

15 后，在此进一步增加附加的条件，即所述元数据服务器根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，当同时满足此附加的条件的时候，才判断为对解开的待访问数据的权限验证通过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不允许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据

20 安全性。详细的，在分布式文件系统中，能力鉴权（Capability）可定义为如下格式：

Length	Signature	ID	Expire	Permissions
--------	-----------	----	--------	-------------

其中：Length 表示 Signarure 的长度；

25 Signature 表示私钥，用于验证 Permissions 是否被篡改；

 ID 表示 Capability 的 ID 号，是唯一的；

Expire 表示该 Capability 的过期时间;

Permissions 表示待访问数据的权限。

本申请用于数据访问的客户端一优选的实施例，所述元数据服务器，用于根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后，在此进一步增加附加的条件，即所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则判断为满足附加的条件，当解开的待访问数据的权限过大，超过所述预设的权限阈值，则判断为不满足附加的条件，当同时满足附加的条件的时候，才判断为对解开的待访问数据的权限验证通过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不充许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全。

本申请用于数据访问的客户端一优选的实施例，所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据；在此，可以在元数据服务器和数据服务器部署相同的密钥（key），例如，可以在元数据服务器和数据服务器部署一个同样的文件（key.txt），该文件里保存着密钥（key），该密钥（key）必须要保存在一个安全的目录，需要特定权限才可以打开，以防止密钥被窃取，密钥（key）的长度可以随机选取，长度不能太短也不能太长，可设定 key 的长度为 16 字节(128 位)，密钥（key）可以使用 linux 操作系统的 uuid 生成，可以通过 /proc/sys/kernel/random/uuid 来随机生成一个 uuid 码，也可以使用 openssl 命令来生成一个密钥 key，另外，客户端请求访问元数据服务器并通过对解开的待访问数据的权限的验证的时候，元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')|msg'|msg, msg 为元数据，其中，msg' 为从所述元数据（msg）中提取的部分元数据，HMAC(key, msg')

为用所述密钥 (key) 并采用 HMAC 算法加密后的部分元数据 (msg'), 元数据可对由密钥加工后的元数据信息进行 protocolbuffer 序列化之后将其发送给客户端, 后续客户再将序列化之后的由密钥加工后的元数据信息发送至数据服务器, 在此, 生成所述用所述密钥加密后的部分元数据的加密算法
5 不限于上述 HMAC 算法, 其中, HMAC 为消息认证码, 其通过捆绑一个共享密钥可以使用任何迭代的可用于加密的散列函数;

所述数据服务器 3, 用于用所述密钥对接收到的所述部分元数据进行本地加密, 并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较, 如果比较一致, 则验证通过; 在此, 数据服务器收到客户端
10 发来的序列化之后的由密钥加工后的元数据信息, 针对接收到的序列化后的信息进行反序列化之后, 从本地部署的文件 (key.txt) 中获取密钥 (key), 利用该 key 值对接收的 msg' 字段进行 HMAC (Hash-based Message Authentication Code) 算法得到 HMAC(key, msg'), 看得到的 HMAC(key, msg') 和接收到的 HMAC(key, msg') 是否一样, 如果一样就可以确定接收到的由密钥加工后的
15 元数据信息是从元数据服务器获取到的, 因为客户端没有密钥 (key), 说明客户端是可信的, 这样, 客户端就可以与数据服务器建立可信连接, 就可以安全地传输待访问数据了;

获取数据装置 13, 用于根据所述元数据从所述数据服务器获取所述待访问数据。

20 本申请用于数据访问的客户端一优选的实施例中, 所述由密钥加工后的元数据信息包括: 元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间; 在此, 以上述元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')|msg'|msg 为例, 可以在用所述密钥加密后的部分元数据 (msg') 中设置元数据的过期时间
25 (expire_time), 如 msg'={FileID, READ / WRITE, expire_time};

所述数据服务器 3, 用于用所述密钥对接收到的所述部分元数据进行本地

加密,并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据
进行比较,并根据所述元数据的过期时间判断元数据是否过期,如果比
较一致且元数据未过期,则验证通过;在此,在将本地加密后得到的结果
与接收到的用所述密钥加密后的部分元数据进行比较,满足比较一致的条
件同时,还需要另一条件,即数据服务器判断元数据未过期,两个条件都
5 满足后,才判断为验证通过,可以进行后续对数据服务器的访问,从而实
现对所述由密钥加工后的元数据信息验证更严格的验证,保证客户端的可
信度,详细的,元数据服务器通过设置客户端访问数据服务器的过期时间
(`expire_time`),一旦这个 `expire_time` 到期之后,数据服务器可以触发一个
10 到期(`token expire`)事件,该到期事件会发个请求给客户端,客户端需
要重新向元数据服务器请求由密钥加工后的元数据信息;

所述获取数据装置 13,用于根据所述元数据从所述数据服务器获取所述待访问数据。

如图 8 所示,根据本申请的另一面,还提供一种辅助数据访问的元数
15 据服务器,该元数据服务器 2 包括:

接收权限装置 21,用于从客户端接收用私钥签发的待访问数据的权限;
具体的,如图 2 所示,分布式文件系统架构由三方来参与的:Client 端
(客户端 1)、NameNode 端(元数据服务器 2)、DataNode 端(数据服务器 3),
这三方的通信可以是基于 RPC 协议来通信,建立在 TCP/IP 协议之上,元数
20 据服务器存储着待访问数据的元数据信息(`meta`),元数据信息用于记录待
访问数据在数据服务器上存储位置的信息,客户端通过从元数据服务器获取
元数据信息,然后通过元数据信息直接访问数据服务器获取所需要的待访问
数据,对于元数据服务器的访问控制可以使用能力鉴权(`Capability`)的方式,
`Capability` 是用于访问控制的一种数据结构,其定义了一个或多个指定的资
25 源(如目录、文件等)所具有的访问权限,能力鉴权需要包括私钥(`Signature`)
和待访问数据的权限(`Permissions`),以便客户端向元数据服务器发送用私

钥签发的待访问数据的权限，在此待访问数据的权限(Permissions)可以是一个权限集合列表，每一个 permission 可以有两个字段：权限集合编号 resourceID 和对应于权限集合编号的权限集合 (permission bundle)，可以根据需要设置权限集合的数据位数，如可设置 32bits，每个 bit 表示用户定义的一个权限，待访问数据的权限可以包括：READ(读权限)、WRITE(写权限)、
5 ROOT(读写权限，等价于 READ|WRITE)；

生成元数据装置 22，用于用公钥解开所述用私钥签发的待访问数据的权限，对解开的待访问数据的权限验证通过后生成由密钥加工后的元数据信息；在此，所述公钥是对应于所述私钥的公钥，以方便所述元数据服务
10 器用公钥解开所述用私钥签发的待访问数据的权限，当客户端去访问元数据服务器的时候，向元数据服务器发送用私钥签发的待访问数据的权限，然后元数据服务器拿到该用私钥签发的待访问数据的权限之后需要作验证，如果验证通过，客户端就可以从元数据服务器获取由密钥加工后的元数据信息，进而继续后续对数据服务器的访问，例如，当客户端 client1 请求读取待访问数据 file1 的内容，RPC 协议下请求格式为：(/client1/file1,
15 READ),客户端会向元数据服务器发送该请求的用私钥签发的待访问数据的权限，这个时候客户端会向元数据服务器发送的消息内容具体可参见图 3，消息内容包括：消息头 (A)、包含具体请求内容的消息体 (B) 及用私钥签发的待访问数据的权限 (C)，客户端可用 protocolbuffer (google 的一种数据交换的格式) 格式来传输消息内容，然后元数据服务器拿到用私钥
20 签发的待访问数据的权限之后，利用公钥解开用私钥签发的待访问数据的权限，然后对解开的待访问数据的权限验证通过后生成所述由密钥加工后的元数据信息，客户端从元数据服务器获取由密钥加工后的元数据信息，其中，所述用私钥签发的待访问数据的权限可由客户端自己生成，也可由
25 另外的第三方生成后，由客户端从所述第三方获取，另外，当客户端能够利用公钥解开用私钥签发的待访问数据的权限，即可判断为对解开的待访问

数据的权限验证通过，也可以在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后，进一步增加附加的条件，当同时满足附加的条件的时候，才判断为对解开的待访问数据的权限验证通过；

5 发送元数据装置 23，用于将所述由密钥加工后的元数据信息发送至所述客户端。本实施例通过所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限，并对解开的待访问数据的权限验证通过后，生成所述由密钥加工后的元数据信息，可以实现对元数据服务器的访问控制，这样可以确保元数据服务器的安全性。

10 如图 9 所示，本申请的辅助数据访问的元数据服务器一优选的实施例中，所述元数据服务器 2 还包括接收过期时间装置 24，用于从所述客户端接收所述待访问数据的权限的过期时间(Expire)；

所述生成元数据装置 22，用于根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，则验证通过。在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后，在此进一步增加附加的条件，15 即所述元数据服务器根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，当同时满足此附加的条件的时候，才判断为对解开的待访问数据的权限验证通过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不充许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全性。详细的，在分布式文件20 系统中，能力鉴权（Capability）可定义为如下格式：

Length	Signature	ID	Expire	Permissions
--------	-----------	----	--------	-------------

其中：Length 表示 Signarure 的长度；

Signature 表示私钥，用于验证 Permissions 是否被篡改；

25 ID 表示 Capability 的 ID 号，是唯一的；

Expire 表示该 Capability 的过期时间；

Permissions 表示待访问数据的权限。

本申请的辅助数据访问的元数据服务器一优选的实施例中，所述生成元数据装置 22，用于根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。在元数据服务器能够利用公钥解
5 开用私钥签发的待访问数据的权限后，在此进一步增加附加的条件，即所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则判断为满足附加的条件，当解开的待访问数据的权限过大，超过所述预设的权限阈值，则判断为不满足附加的条件，当同时满足附加的条件的时候，才判断为对解开的待访问数据的权限验证通
10 过，进而更严格地对待访问数据的权限进行验证，对不满足附加条件的情况，则不充许客户端后续对数据服务器的访问，保证后续需要访问的数据服务器上的数据安全性。

本申请的辅助数据访问的元数据服务器一优选的实施例中，所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据
15 及用所述密钥加密后的部分元数据。在此，可以在元数据服务器和数据服务器部署相同的密钥（key），例如，可以在元数据服务器和数据服务器部署一个同样的文件（key.txt），该文件里保存着密钥（key），该密钥（key）必须要保存在一个安全的目录，需要特定权限才可以打开，以防止密钥被窃取，密钥（key）的长度可以随机选取，长度不能太短也不能太长，可
20 设定 key 的长度为 16 字节(128 位)，密钥（key）可以使用 linux 操作系统的 uuid 生成，可以通过 /proc/sys/kernel/random/uuid 来随机生成一个 uuid 码，也可以使用 openssl 命令来生成一个密钥 key，另外，客户端请求访问元数据服务器并通过对解开的待访问数据的权限的验证的时候，元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')\msg'\msg, msg 为元
25 数据，其中，msg'为从所述元数据（msg）中提取的部分元数据，HMAC(key, msg')为用所述密钥（key）并采用 HMAC 算法加密后的部分元数据（msg'），

元数据可对由密钥加工后的元数据信息进行 protocolbuffer 序列化之后将其发送给客户端，后续客户再将序列化之后的由密钥加工后的元数据信息发送至数据服务器，在此，生成所述用所述密钥加密后的部分元数据的加密算法不限于上述 HMAC 算法，其中，HMAC 为消息认证码，其通过捆绑一个共享密钥可以使用任何迭代的可用于加密的散列函数。

本申请的辅助数据访问的元数据服务器一优选的实施例中，所述由密钥加工后的元数据信息还包括：元数据的过期时间。在此，以上述元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')\msg'\msg 为例，可以在用所述密钥加密后的部分元数据 (msg') 中设置元数据的过期时间 (expire_time)，如 msg'={FileID, READ / WRITE, expire_time}。

如图 10 所示，根据本申请的另一面，还提供一种辅助数据访问的数据服务器，该数据服务器 3 包括：

元数据装置 31，用于从客户端获取由密钥加工后的元数据信息；

验证装置 32，用于通过所述密钥对所述由密钥加工后的元数据信息进行验证；

数据传输装置 33，用于对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据。本实施例在所述数据服务器对所述由密钥加工后的元数据信息验证通过后，才允许客户端从所述数据服务器获取所述待访问数据，可以实现对数据服务器的访问控制，这样可以确保数据服务器的安全性，最终实现客户端的抗伪造性。

本申请的辅助数据访问的数据服务器的一优选的实施例中，当所述元数据信息包括元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据时，所述数据传输装置 33，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，如果比较一致，则验证通过；根据所述元数据向所述客户端传输所述待访问数据。在此，可以在元数据服务器

和数据服务器部署相同的密钥 (key), 例如, 可以在元数据服务器和数据服务器部署一个同样的文件 (key.txt), 该文件里保存着密钥 (key), 该密钥 (key) 必须要保存在一个安全的目录, 需要特定权限才可以打开, 以防止密钥被窃取, 密钥 (key) 的长度可以随机选取, 长度不能太短也不能太长, 可设定 key 的长度为 16 字节(128 位), 密钥 (key) 可以使用 linux 操作系统的 uuid 生成, 可以通过 /proc/sys/kernel/random/uuid 来随机生成一个 uuid 码, 也可以使用 openssl 命令来生成一个密钥 key, 另外, 客户端请求访问元数据服务器并通过对解开的待访问数据的权限的验证的时候, 元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')lmsg'lmsg, msg 为元数据, 其中, msg' 为从所述元数据 (msg) 中提取的部分元数据, HMAC(key, msg') 为用所述密钥 (key) 并采用 HMAC 算法加密后的部分元数据 (msg'), 元数据可对由密钥加工后的元数据信息进行 protocolbuffer 序列化之后将其发送给客户端, 后续客户再将序列化之后的由密钥加工后的元数据信息发送至数据服务器, 在此, 生成所述用所述密钥加密后的部分元数据的加密算法不限于上述 HMAC 算法, 其中, HMAC 为消息认证码, 其通过捆绑一个共享密钥可以使用任何迭代的可用于加密的散列函数, 数据服务器收到客户端发来的序列化之后的由密钥加工后的元数据信息, 针对接收到的序列化后的信息进行反序列化之后, 从本地部署的文件 (key.txt) 中获取密钥 (key), 利用该 key 值对接收到的 msg' 字段进行 HMAC (Hash-based Message Authentication Code) 算法得到 HMAC(key, msg'), 看得到的 HMAC(key, msg') 和接收到的 HMAC(key, msg') 是否一样, 如果一样就可以确定接收到的由密钥加工后的元数据信息是从元数据服务器获取到的, 因为客户端没有密钥 (key), 说明客户端是可信的, 这样, 客户端就可以与数据服务器建立可信连接, 就可以安全地传输待访问数据了。

本申请的辅助数据访问的数据服务器的一优选的实施例, 当所述由密钥加工后的元数据信息包括: 元数据、从所述元数据中提取的部分元

数据、用所述密钥加密后的部分元数据及元数据的过期时间时，所述数据传输装置 33，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则验证通过；根据所述元数据向所述客户端传输所述待访问数据。在此，以上述元数据服务器返回给客户端的元数据信息包括 HMAC(key, msg')\msg'\msg 为例，可以在用所述密钥加密后的部分元数据(msg')中设置元数据的过期时间(expire_time)，如 msg'={FileID, READ / WRITE, expire_time}，在将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，满足比较一致的条件同时，还需要另一条件，即数据服务器判断元数据未过期，两个条件都满足后，才判断为验证通过，可以进行后续对数据服务器的访问，从而实现对所述由密钥加工后的元数据信息验证更严格的验证，保证客户端的可信度，详细的，元数据服务器通过设置客户端访问数据服务器的过期时间(expire_time)，一旦这个 expire_time 到期之后，数据服务器可以触发一个到期(token expire)事件，该到期事件会发个请求给客户端，客户端需要重新向元数据服务器请求由密钥加工后的元数据信息。

详细的，如图 11 所示，本申请一具体的应用实施例包括如下步骤：

步骤 S111，客户端向元数据服务器发送用私钥签发的待访问数据的权限；

步骤 S112，所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限，并对解开的待访问数据的权限验证通过后生成由密钥加工后的元数据信息；

步骤 S113，所述客户端从所述元数据服务器获取所述由密钥加工后的元数据信息，并将所述由密钥加工后的元数据信息发送至数据服务器；

步骤 S114，所述数据服务器通过所述密钥对所述由密钥加工后的元数

据信息进行验证;

步骤 S115, 待所述数据服务器对所述由密钥加工后的元数据信息验证通过后, 所述客户端从所述数据服务器获取所述待访问数据。

综上所述, 本申请通过所述元数据服务器用公钥解开所述用私钥签发的待访问数据的权限, 并对解开的待访问数据的权限验证通过后, 生成所述由密钥加工后的元数据信息, 可以实现对元数据服务器的访问控制, 这样可以确保元数据服务器的安全性, 另外, 在所述数据服务器对所述由密钥加工后的元数据信息验证通过后, 才允许客户端从所述数据服务器获取所述待访问数据, 可以实现对数据服务器的访问控制, 这样可以确保数据服务器的安全性, 最终实现客户端的抗伪造性。

进一步的, 本申请在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后, 进一步增加附加的条件, 即所述元数据服务器根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时, 当同时满足此附加的条件的时候, 才判断为对解开的待访问数据的权限验证通过, 进而更严格地对待访问数据的权限进行验证, 对不满足附加条件的情况, 则不允许客户端后续对数据服务器的访问, 保证后续需要访问的数据服务器上的数据安全性。

进一步的, 本申请在元数据服务器能够利用公钥解开用私钥签发的待访问数据的权限后, 进一步增加附加的条件, 即所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时, 则判断为满足附加的条件, 当解开的待访问数据的权限过大, 超过所述预设的权限阈值, 则判断为不满足附加的条件, 当同时满足附加的条件的时候, 才判断为对解开的待访问数据的权限验证通过, 进而更严格地对待访问数据的权限进行验证, 对不满足附加条件的情况, 则不允许客户端后续对数据服务器的访问, 保证后续需要访问的数据服务器上的数据安全性。

进一步的, 本申请中所述数据服务器用所述密钥对接收到的所述部分无

数进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，在如果比较一致，才验证通过，因为客户端没有密钥（key），说明客户端是可信的，这样，客户端就可以与数据服务器建立可信连接，就可以安全地传输待访问数据。

5 进一步的，本申请中所述数据服务器用所述密钥对接收到的所述部分无数进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，满足比较一致的条件同时，还需要另一条件，即数据服务器判断元数据未过期，两个条件都满足后，才判断为验证通过，可以进行后续对数据服务器的访问，从而实现对所述由密钥加工后的元数据信息验证更严格的验证，保证客户端的可信度。

10 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在

15 内。

 需要注意的是，本发明可在软件和/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，本发明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，本发明的软件程序（包括相关的数据结构）

20 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，本发明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。

 另外，本发明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

25 根据本发明的方法和/或技术方案。而调用本发明的方法的程序指令，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，根据本发明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发明的多个实施例的方法和/或技术方案。

对于本领域技术人员而言，显然本发明不限于上述示范性实施例的细节，而且在不背离本发明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发明。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，本发明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发明内。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。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

权 利 要 求 书

1. 一种客户端用于数据访问的方法，其中，该方法包括：

向元数据服务器发送用私钥签发的待访问数据的权限；

从元数据服务器获取由密钥加工后的元数据信息，其中，所述用私钥
5 签发的待访问数据的权限由所述元数据服务器用公钥解开，所述由密钥加
工后的元数据信息由所述元数据服务器对解开的待访问数据的权限验证
通过后生成；

将所述由密钥加工后的元数据信息发送至数据服务器，待所述数据服务
器对所述由密钥加工后的元数据信息验证通过后，从所述数据服务器获取
10 所述待访问数据，其中，所述由密钥加工后的元数据信息由所述数据服务
器通过所述密钥进行验证。

2. 如权利要求 1 所述的方法，其中，向元数据服务器发送用私钥签发的
的待访问数据的权限的同时，还包括：

向元数据服务器发送所述待访问数据的权限的过期时间；

15 所述元数据服务器对解开的待访问数据的权限验证通过，包括：

所述元数据服务器根据所述权限的过期时间对解开的待访问数据的
权限判断为未过期时，则验证通过。

3. 如权利要求 1 或 2 所述的方法，其中，所述元数据服务器对解开的
待访问数据的权限验证通过，包括：

20 所述元数据服务器根据预设的权限阈值对解开的待访问数据的权限
判断为未超过所述权限阈值时，则验证通过。

4. 如权利要求 1 至 3 任一项所述的方法，其中，所述由密钥加工后的
元数据信息包括：

元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部
25 分元数据；

所述数据服务器对所述由密钥加工后的元数据信息验证通过，包括：

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密,并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较,如果比较一致,则验证通过;

从所述数据服务器获取所述待访问数据,包括:

5 根据所述元数据从所述数据服务器获取所述待访问数据。

5. 如权利要求 1 至 3 任一项所述的方法,其中,所述由密钥加工后的元数据信息包括:

元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间;

10 所述数据服务器对所述由密钥加工后的元数据信息验证通过,包括:

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密,并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较,并根据所述元数据的过期时间判断元数据是否过期,如果比较一致且元数据未过期,则验证通过;

15 从所述数据服务器获取所述待访问数据,包括:

根据所述元数据从所述数据服务器获取所述待访问数据。

6. 一种元数据服务器端用于辅助数据访问的方法,其中,该方法包括:

从客户端接收用私钥签发的待访问数据的权限;

20 用公钥解开所述用私钥签发的待访问数据的权限,对解开的待访问数据的权限验证通过后生成由密钥加工后的元数据信息;

将所述由密钥加工后的元数据信息发送至所述客户端。

7. 如权利要求 6 所述的方法,其中,从客户端接收用私钥签发的待访问数据的权限的同时,还包括:

从所述客户端接收所述待访问数据的权限的过期时间;

25 对解开的待访问数据的权限验证通过,包括:

根据所述权限的过期时间对解开的待访问数据的权限判断为未过期

时，则验证通过。

8. 如权利要求 6 或 7 所述的方法，其中，对解开的待访问数据的权限验证通过，包括：

根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述
5 权限阈值时，则验证通过。

9. 如权利要求 6 至 8 任一项所述的方法，其中，所述由密钥加工后的元数据信息包括：

元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据。

10 10. 如权利要求 9 所述的方法，其中，所述由密钥加工后的元数据信息还包括：

元数据的过期时间。

11. 一种数据服务器端用于辅助数据访问的方法，其中，该方法包括：
从客户端获取由密钥加工后的元数据信息；

15 通过所述密钥对所述由密钥加工后的元数据信息进行验证；

对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据。

12. 如权利要求 11 所述的方法，其中，当所述元数据信息包括元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据时，
20 对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据，包括：

用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，如果比较一致，则验证通过；

25 根据所述元数据向所述客户端传输所述待访问数据。

13. 如权利要求 12 所述的方法，其中，当所述由密钥加工后的元数据

信息包括：元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间时，对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据，包括：

所述数据服务器用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则验证通过；

根据所述元数据向所述客户端传输所述待访问数据。

14. 一种用于数据访问的客户端，其中，该客户端包括：

10 发送权限装置，用于向元数据服务器发送用私钥签发的待访问数据的权限；

获取元数据装置，用于从元数据服务器获取由密钥加工后的元数据信息，其中，所述用私钥签发的待访问数据的权限由所述元数据服务器用公钥解开，所述由密钥加工后的元数据信息由所述元数据服务器对解开的待访问数据的权限验证通过后生成；

15 获取数据装置，用于将所述由密钥加工后的元数据信息发送至数据服务器，待所述数据服务器对所述由密钥加工后的元数据信息验证通过后，从所述数据服务器获取所述待访问数据，其中，所述由密钥加工后的元数据信息由所述数据服务器通过所述密钥进行验证。

20 15. 如权利要求 14 所述的客户端，其中，所述客户端还包括发送过期时间装置，用于在向元数据服务器发送用私钥签发的待访问数据的权限的同时，向元数据服务器发送所述待访问数据的权限的过期时间，其中，所述元数据服务器，用于根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，则验证通过。

25 16. 如权利要求 14 或 15 所述的客户端，其中，所述元数据服务器，用于根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述

权限阈值时，则验证通过。

17. 如权利要求 14 至 16 任一项所述的客户端，其中，所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据；

5 所述数据服务器，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，如果比较一致，则验证通过；

获取数据装置，用于根据所述元数据从所述数据服务器获取所述待访问数据。

10 18. 如权利要求 14 至 16 任一项所述的客户端，其中，所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据、用所述密钥加密后的部分元数据及元数据的过期时间；

所述数据服务器，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据
15 据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则验证通过；

所述获取数据装置，用于根据所述元数据从所述数据服务器获取所述待访问数据。

19. 一种辅助数据访问的元数据服务器，其中，该元数据服务器包括：
20 接收权限装置，用于从客户端接收用私钥签发的待访问数据的权限；
生成元数据装置，用于用公钥解开所述用私钥签发的待访问数据的权限，对解开的待访问数据的权限验证通过后生成由密钥加工后的元数据信息；

发送元数据装置，用于将所述由密钥加工后的元数据信息发送至所述
25 客户端。

20. 如权利要求 19 所述的元数据服务器，其中，所述元数据服务器还

包括接收过期时间装置，用于从所述客户端接收所述待访问数据的权限的过期时间；

所述生成元数据装置，用于根据所述权限的过期时间对解开的待访问数据的权限判断为未过期时，则验证通过。

5 21. 如权利要求 19 或 20 所述的元数据服务器，其中，所述生成元数据装置，用于根据预设的权限阈值对解开的待访问数据的权限判断为未超过所述权限阈值时，则验证通过。

22. 如权利要求 19 至 21 任一项所述的元数据服务器，其中，所述由
10 密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据。

23. 如权利要求 22 所述的元数据服务器，其中，所述由密钥加工后的元数据信息还包括：元数据的过期时间。

24. 一种辅助数据访问的数据服务器，其中，该数据服务器包括：

元数据装置，用于从客户端获取由密钥加工后的元数据信息；

15 验证装置，用于通过所述密钥对所述由密钥加工后的元数据信息进行验证；

数据传输装置，用于对所述由密钥加工后的元数据信息验证通过后，向所述客户端传输所述待访问数据。

25 25. 如权利要求 24 所述的数据服务器，其中，当所述元数据信息包括元数据、从所述元数据中提取的部分元数据及用所述密钥加密后的部分元数据时，所述数据传输装置，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，如果比较一致，则验证通过；根据所述元数据向所述客户端传输所述待访问数据。

26. 如权利要求 25 所述的数据服务器，其中，当所述由密钥加工后的元数据信息包括：元数据、从所述元数据中提取的部分元数据、用所述密

- 钥加密后的部分元数据及元数据的过期时间时，所述数据传输装置，用于用所述密钥对接收到的所述部分元数据进行本地加密，并将本地加密后得到的结果与接收到的用所述密钥加密后的部分元数据进行比较，并根据所述元数据的过期时间判断元数据是否过期，如果比较一致且元数据未过期，则
- 5 验证通过；根据所述元数据向所述客户端传输所述待访问数据。

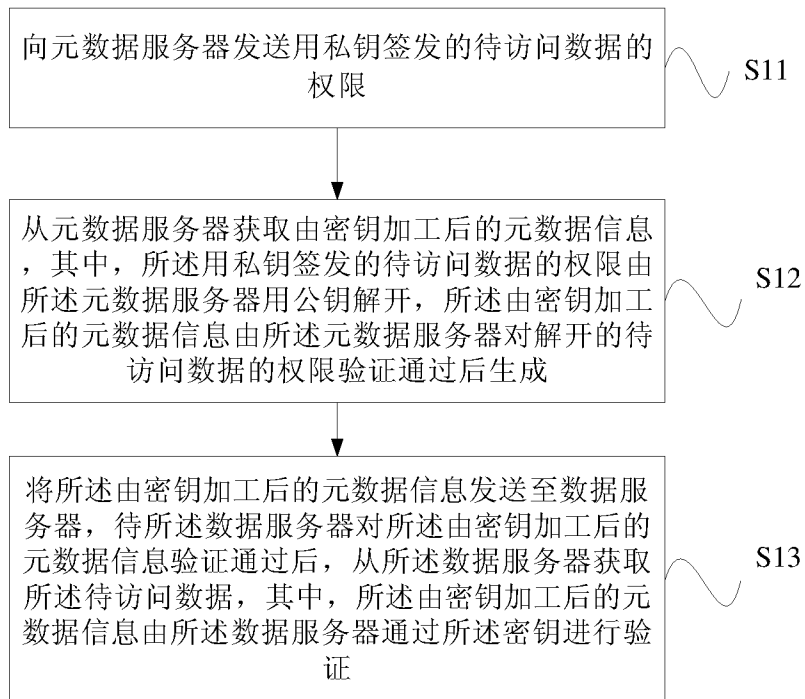


图 1

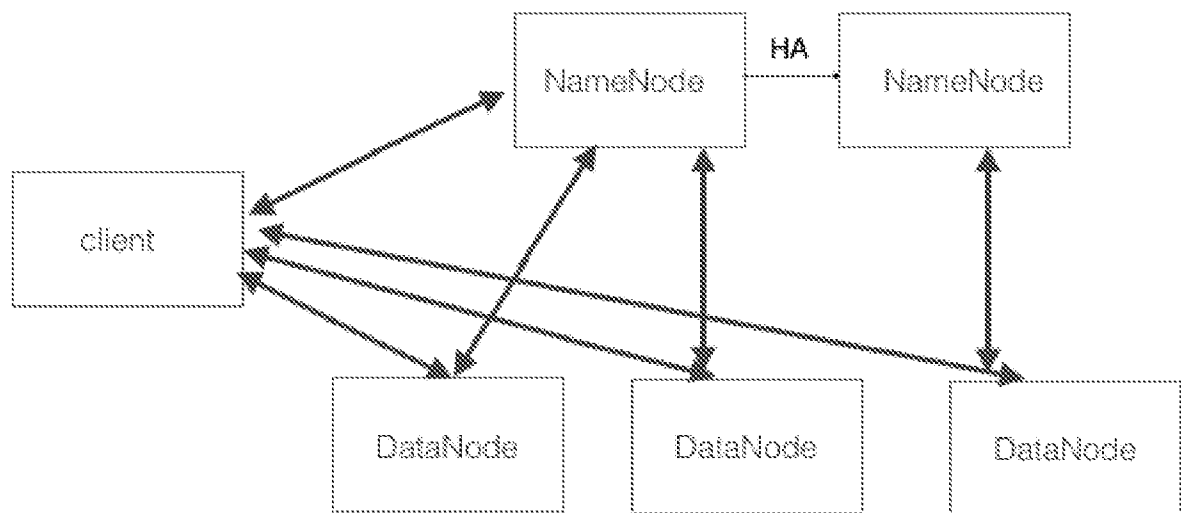


图 2

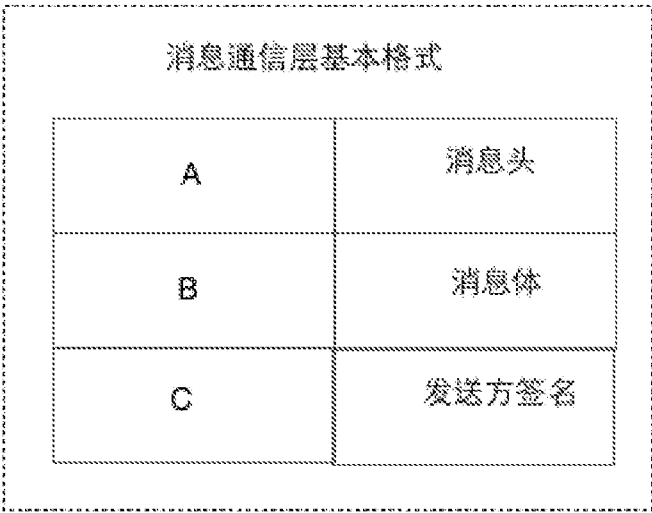


图 3

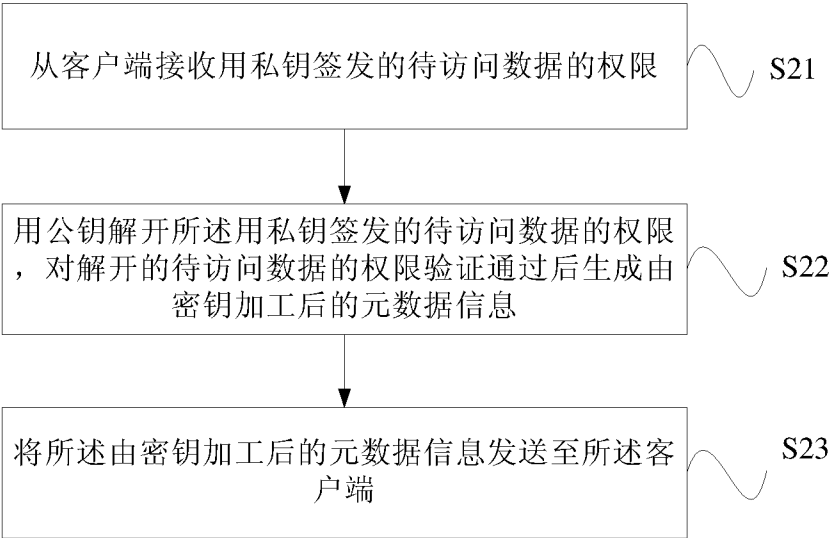


图 4

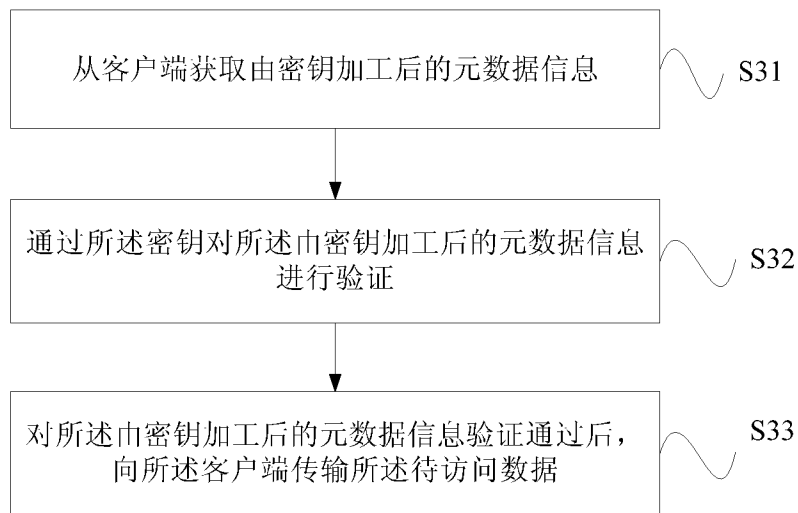


图 5

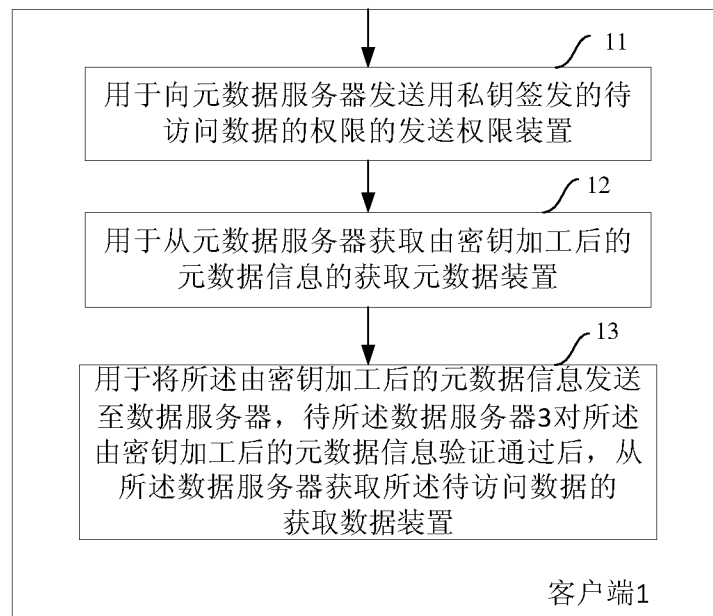


图 6

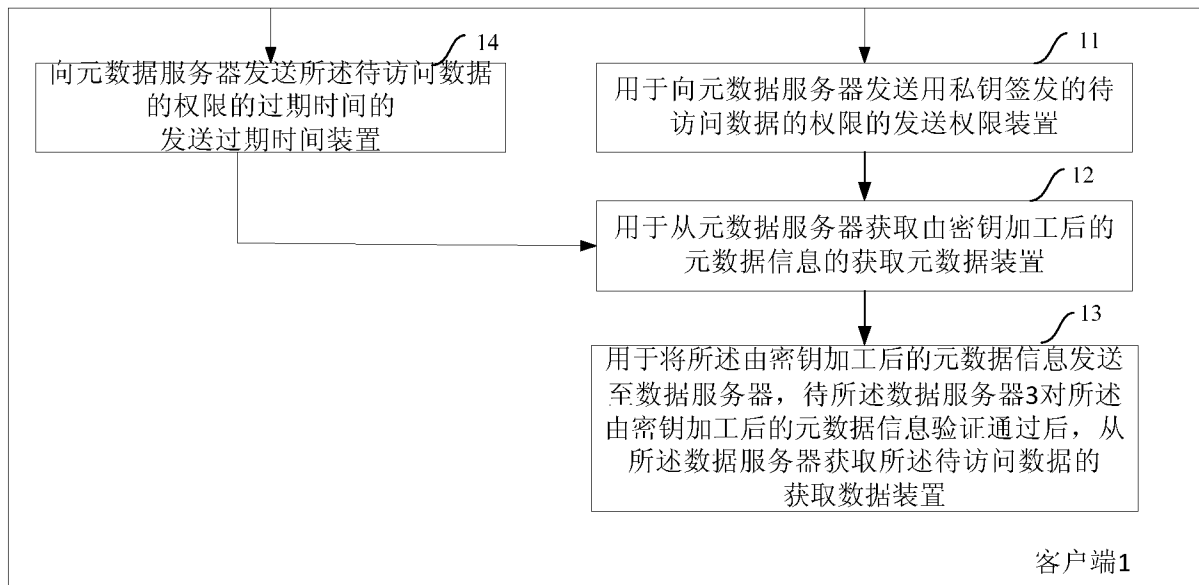


图 7

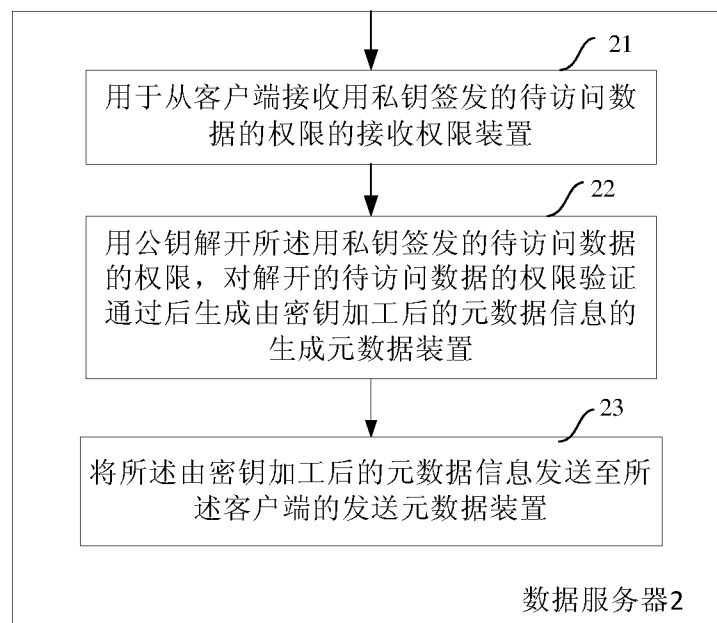


图 8

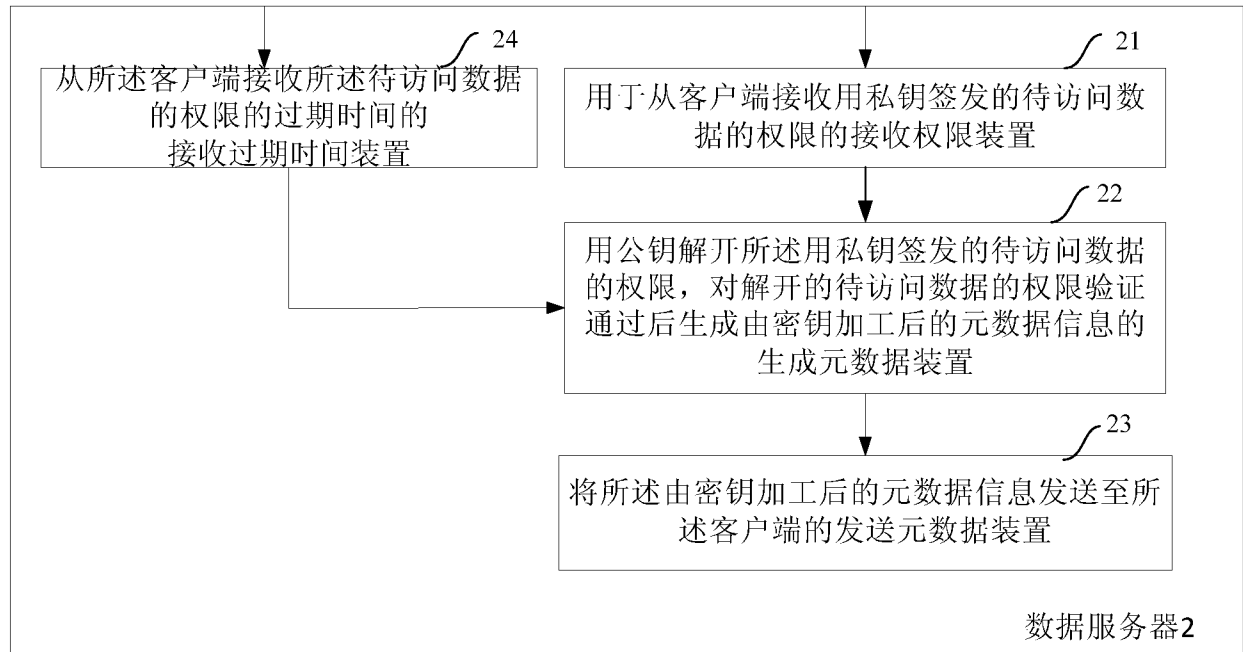


图 9

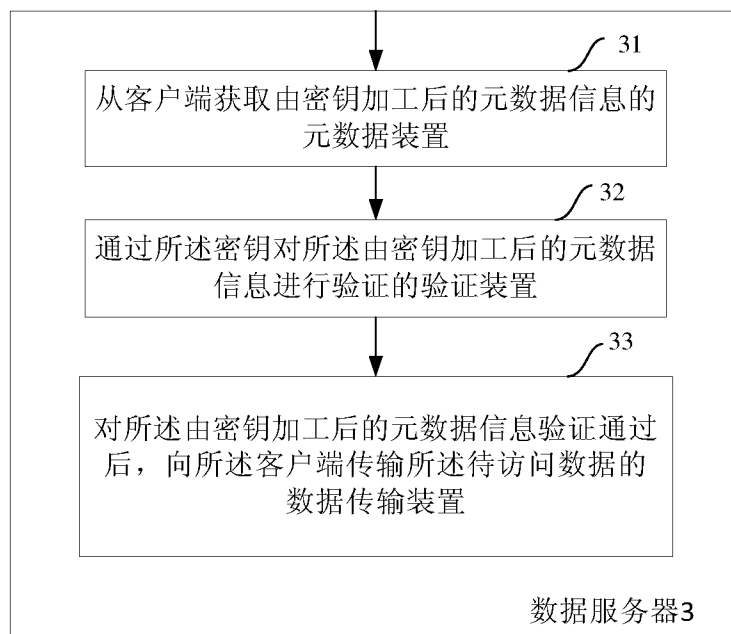


图 10

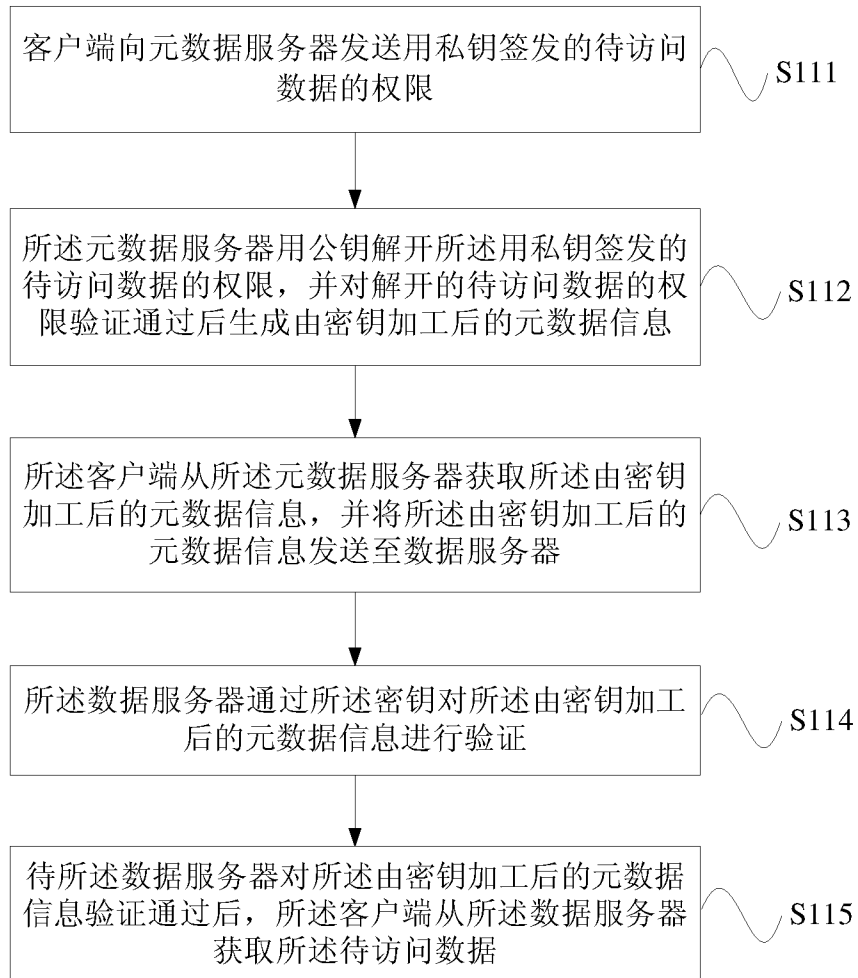


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/090821

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) 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)

H04W H04L H04Q G06F

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, CNKI, WPI, EPODOC: distributed file system, HDFS, metadata, capacity authentication, meta, permission, authority, read, write, capability, security, validat+, verif+, key, encrypt+, public key, private key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102457561 A (JIANGNAN INSTITUTE OF COMPUTING TECHNOLOGY), 16 May 2012 (16.05.2012), description, paragraphs [0072]-[0082], figures 4 and 5	11, 24
A	CN 104580487 A (CHENGDU SCENE TECHNOLOGY CO., LTD.), 29 April 2015 (29.04.2015), the whole document	1-26
A	CN 102546664 A (INSTITUTE OF COMPUTING TECHNOLOGY, CHINESE ACADEMY OF SCIENCES), 04 July 2012 (04.07.2012), the whole document	1-26
A	CN 103488755 A (HUAWEI TECHNOLOGIES CO., LTD.), 01 January 2014 (01.01.2014), the whole document	1-26
A	US 2013151884 A1 (PROMISE TECHNOLOGY, INC.), 13 June 2013 (13.06.2013), the whole document	1-26

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 20 September 2016 (20.09.2016)	Date of mailing of the international search report 25 October 2016 (25.10.2016)
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 WANG, Jimei Telephone No.: (86-10) 62413363

International application No.
PCT/CN2016/090821

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 H04L 9/32 (2006.01) 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) H04W H04L H04Q G06F 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, CNKI, WPI, EPDOC: 分布式文件系统, HDFS, 元数据, 权限, 读, 写, 能力鉴权, 安全, 验证, 密钥, 加密, 公钥, 私钥; meta, permission, authority, read, write, capability, security, validat+, verif+, key, encrypt+, public key, private key		
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
X	CN 102457561 A (无锡江南计算技术研究所) 2012年 5月 16日 (2012 - 05 - 16) 说明书第[0072]-[0082]段, 附图4, 5	11, 24
A	CN 104580487 A (成都信升斯科技有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-26
A	CN 102546664 A (中国科学院计算技术研究所) 2012年 7月 4日 (2012 - 07 - 04) 全文	1-26
A	CN 103488755 A (华为技术有限公司) 2014年 1月 1日 (2014 - 01 - 01) 全文	1-26
A	US 2013151884 A1 (PROMISE TECHNOLOGY, INC.) 2013年 6月 13日 (2013 - 06 - 13) 全文	1-26
☐ 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 2016年 9月 20日		国际检索报告邮寄日期 2016年 10月 25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 王继梅 电话号码 (86-10) 62413363

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/090821

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	102457561	A	2012年 5月 16日	无	
CN	104580487	A	2015年 4月 29日	无	
CN	102546664	A	2012年 7月 4日	无	
CN	103488755	A	2014年 1月 1日	无	
US	2013151884	A1	2013年 6月 13日	TW 201324183 A	2013年 6月 16日