(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
2014 年 8 月 7 日 (07.08.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/117649 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2014/070724

(22) 国际申请日: 2014 年 1 月 16 日 (16.01.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310035962.6 2013 年 1 月 30 日 (30.01.2013) CN

(71) 申请人: **华为终端有限公司 (HUAWEI DEVICE CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地 B 区 2 号楼, Guangdong 518129 (CN)。

(72) 发明人: **汪婵 (WANG, Chan)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **黄洁静 (HUANG, Jiejing)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **吴黄伟 (WU, Huangwei)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, LT, 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, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,

[见续页]

(54) **Title**: METHOD AND APPARATUS FOR DATA SHARING

(54) **发明名称**: 一种数据共享的方法及装置

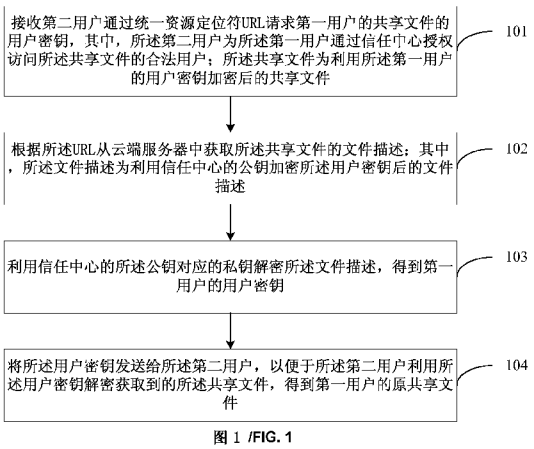

图 1 /FIG. 1

101 Receiving an user key of a shared file of a first user which is requested by a second user using a Uniform Resource Locator (URL), wherein the second user is a legal user authorized by the first user through a trust center to access the shared file, and the shared file is the shared file which is encrypted using the user key of the first user

102 Obtaining the file description of the shared file from a cloud end server according to the URL, wherein the file description is the file description after encrypting the user key using the public key of the trust center

103 Decrypting the file description using the corresponding private key of the public key of the trust center , and obtaining the user key of the first user

104 Sending the user key to the second user, so that the second user decrypts the obtained shared file by using the user key, and gets the original shared file of the first user

(57) **Abstract**: A method includes: receiving an user key of a shared file of a first user which is requested by a second user using a Uniform Resource Locator (URL), wherein the second user is a legal user authorized by the first user through a trust center to access the shared file, and the shared file is the shared file which is encrypted using the user key of the first user; obtaining the corresponding file description of the shared file from a cloud end server according to the URL, wherein the file description is the file description after encrypting the user key using the public key of the trust center; decrypting the file description by using the corresponding private key of the public key of the trust center, and obtaining the user key of the first user; sending the user key to the second user.

(57) **摘要**: 一种方法包括：接收第二用户通过统一资源定位符 URL 请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用第一用户的用户密钥加密后的共享文件；根据所述 URL 从云端服务器中获取对应的所述共享文件的文件描述；其中，所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；利用信任中心的所述公钥对应的私钥解密所述文件描述，得到第一用户的用户密钥；将所述用户密钥发送给所述第二用户。

WO 2014/117649 A1

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))。

一种数据共享的方法及装置

[01] 本申请要求于 2013 年 1 月 30 日提交中国专利局、申请号为 201310035962.6、发明名称为“一种数据共享的方法及装置”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。

技术领域

[02] 本发明涉及网络技术领域，特别涉及一种数据共享的方法及装置。

背景技术

[03] 随着网络技术的发展，越来越多的企业和个人愿意将自己的数据上传到云端来降低存储成本。云服务提供商（或云端服务器）会方便地替用户处理很多事情，例如，数据共享、数据备份等等。在对数据共享和数据备份的同时，安全问题是用户最关注的一个问题，也是目前云服务提供商面临的最大挑战。如果用户不信任云服务提供商，数据在上传到云端之前将被加密。因此，云环境下，如何将云端服务器上的数据安全共享给其他用户，将是目前要解决的问题。

[04] 现有技术中，如果用户想共享上传到云端服务提供商的服务器上的数据，需要在不同的服务提供商的服务器中设置数据的共享权限，允许其他用户访问。并且，在其他用户要想取得共享数据时，需要登录到不同的服务提供商的服务器上，依次通过不同的服务提供商的服务器设置的权限，才能获取到用户共享的数据。

[05] 在对现有技术的研究和实践过程中可知，用户不能灵活的共享云端服务器上的数据，只有通过登录不同服务提供商的服务器提供的服务站点，才能获得相应的服务提供商在云端服务器上存储的共享数据，因此，由于用户需要依次登录到相应的服务站点，才能访问到共享数据，从而导致不能安全方便的访问共享数据。

发明内容

[06] 本发明实施例中提供了一种数据共享的方法及装置，以解决现有技术中用户不能安全方便的访问云端服务器上的数据的技术问题。

[07] 为了解决上述技术问题，本发明实施例公开了如下技术方案：

[08] 第一方面提供了一种数据共享的方法，包括：

[09] 接收第二用户通过统一资源定位符URL请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用所述用户密钥加密后的共享文件；

[10] 根据所述URL从云端服务器中获取对应的所述共享文件的文件描述；其中，所述文件描述为利用所述信任中心的公钥加密所述用户密钥后的文件描述；

[11] 利用所述信任中心的所述公钥对应的私钥解密所述文件描述，得到所述第一用户的所述用户密钥；

[12] 将所述用户密钥发送给所述第二用户。

[13] 在第一方面的第一种可能的实现方式中，所述根据所述URL从云端服务器中获取所述共享文件的文件描述，还包括：

[14] 获取与所述URL对应的所述共享文件；

[15] 利用所述用户密钥解密获取的所述共享文件，得到所述第一用户的原共享文件；

[16] 利用临时密钥加密所述原共享文件，得到临时文件；

[17] 将所述临时文件上传到所述云端服务器中，并获得所述云端服务器下发的与所述临时文件对应的临时URL；

[18] 所述将用户密钥发送给所述第二用户，具体包括：

[19] 将所述临时URL及临时密钥发送给所述第二用户。

[20] 第二方面提供了一种数据共享的方法，所述方法包括：

[21] 利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对所述用户密钥进行加密，并将加密后的用户密钥作为文件描述；

[22] 将加密后的所述共享文件和文件描述上传到所述云端服务器；

[23] 接收所述云端服务器发送的所述共享文件对应的统一资源定位符URL；

[24] 通过所述信任中心授权第二用户访问所述共享文件；

[25] 将所述URL发送给所述第二用户；以便于所述第二用户根据所述URL获取所述用户密钥；并利用所述用户密钥解密所述共享文件。

[26] 在第二方面的第一种可能的实现方式中，

[27] 所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件，具体包括：

[28] 所述第二用户根据所述 URL 从所述信任中心获取所述共享文件的所述用户密钥，以及从所述云端服务器获取所述共享文件，并利用所述用户密钥解密所述共享文件。

[29] 结合第二方面或第二方面第一种可能的实现方式，在第二种可能的实现方式中，

[30] 所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件，具体包括：

[31] 所述第二用户向所述信任中心请求所述 URL 对应的所述共享文件的所述用户密钥；

[32] 接收所述信任中心响应所述请求发送的临时 URL 和临时密钥；其中，所述临时密钥是信任中心对获得的所述共享文件解密后进行重新加密的密钥，所述临时 URL 是云端服务器返回临时文件对应的 URL，其中，所述临时文件为所述信任中心利用所述临时密钥对获得所述共享文件解密后重新加密后的文件；

[33] 向云端服务器获取所述临时 URL 对应的临时文件；

[34] 利用所述临时密钥对所述临时文件进行解密。

[35] 第三方面提供了一种数据共享的方法，所述方法包括：

[36] 接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

[37] 存储所述共享文件及对应的文件描述；

[38] 向所述第一用户发送存储所述共享文件对应的统一资源定位符 URL；

[39] 接收信任中心发送的获取所述 URL 对应的文件描述的请求；

[40] 向所述信任中心发送包括所述文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，以及所述信任中心将所述用户密钥发送给第二用户；

[41] 接收第二用户发送请求所述 URL 对应的共享文件；所述第二用户为所述第一用户通

过所述信任中心授权访问所述共享文件的用户；

[42] 向所述第二用户发送所述 URL 对应的共享文件，以便于所述第二用户根据接收到的所述用户密钥解密所述共享文件。

[43] 第四方面提供了一种数据共享的方法，所述方法包括：

[44] 接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

[45] 存储所述共享文件及对应的文件描述；

[46] 向所述第一用户发送存储所述共享文件和对应的文件描述对应的统一资源定位符 URL；

[47] 接收信任中心发送的获取所述 URL 对应的共享文件和文件描述的请求；

[48] 向所述信任中心发送包括所述共享文件和文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，并利用所述用户密钥解密所述共享文件后利用临时密钥重新加密，得到临时文件；

[49] 接收所述信任中心发送的临时文件；

[50] 存储所述临时文件；

[51] 向所述信任中心发送存储所述临时文件对应的临时 URL；以便于所述信任中心将所述临时密钥和临时 URL 发送给第二用户；

[52] 接收所述第二用户发送的获取所述临时 URL 对应的临时文件的请求；

[53] 向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件。

[54] 第五方面提供了一种数据共享的装置，包括：

[55] 第一接收单元，用于接收第二用户通过统一资源定位符 URL 请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用所述第一用户的用户密钥加密后的共享文件；

[56] 获取单元，用于根据所述 URL 从云端服务器中获取对应的所述共享文件的文件描述；

其中，所述文件描述为利用所述信任中心的公钥加密所述用户密钥后的文件描述；

[57] 第一解密单元，用于利用所述信任中心的所述公钥对应的私钥解密所述文件描述，得到所述第一用户的用户密钥；

[58] 第一发送单元，用于将所述用户密钥发送给所述第二用户。

[59] 在第五方面的第一种可能的实现方式中，

[60] 所述获取单元还用于：在根据所述 URL 从云端服务器中获取所述共享文件的文件描述时，还获取与所述 URL 对应的所述共享文件；所述装置还包括：

[61] 第二解密单元，用于利用所述第一解密单元得到的所述用户密钥解密获取的所述共享文件，得到第一用户的原共享文件；

[62] 加密单元，用于利用临时密钥加密所述原共享文件，得到临时文件；

[63] 第二发送单元，用于将所述临时文件上传到所述云端服务器中；

[64] 第二接收单元，用于所述云端服务器下发的与所述临时文件对应的临时 URL；

[65] 所述第一发送单元，还用于将所述临时 URL 及临时密钥发送给所述第二用户。

[66] 第六方面提供了一种数据共享的装置，包括：

[67] 加密单元，用于利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对所述用户密钥进行加密，并将加密后的用户密钥作为文件描述；

[68] 第一发送单元，用于将加密后的所述共享文件和文件描述上传到所述云端服务器；

[69] 第一接收单元，用于接收所述云端服务器发送的所述共享文件对应的统一资源定位符 URL；

[70] 授权单元，用于通过所述信任中心授权第二用户访问所述共享文件；

[71] 第二发送单元，用于将所述 URL 发送给所述第二用户；以便于所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件。

[72] 第七方面提供了一种数据共享的装置，包括：

[73] 第一接收单元，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

[74] 存储单元，用于存储所述共享文件及对应的文件描述；

[75] 第一发送单元，用于向所述第一用户发送存储所述共享文件对应的统一资源定位符URL；

[76] 第二接收单元，用于接收信任中心发送的获取所述 URL 对应的文件描述的请求；

[77] 第二发送单元，用于向所述信任中心发送包括所述文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，以及所述信任中心将所述用户密钥发送给第二用户；

[78] 第三接收单元，用于接收第二用户发送请求所述 URL 对应的共享文件；所述第二用户为所述第一用户通过所述信任中心授权访问所述共享文件的用户；

[79] 第三发送单元，用于向所述第二用户发送所述 URL 对应的共享文件，以便于所述第二用户根据接收到的所述用户密钥解密所述共享文件。

[80] 第八方面提供了一种数据共享的装置，包括：

[81] 第一接收单元，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

[82] 第一存储单元，用于存储所述共享文件及对应的文件描述；

[83] 第一发送单元，用于向所述第一用户发送存储所述共享文件和文件描述对应的统一资源定位符 URL；

[84] 第二接收单元，用于接收信任中心发送的获取所述 URL 对应的共享文件和文件描述的请求；

[85] 第二发送单元，用于向所述信任中心发送包括所述共享文件和文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，并利用所述用户密钥解密所述共享文件后利用临时密钥重新加密，得到临时文件；

[86] 第三接收单元，用于接收所述信任中心发送的临时文件；

[87] 第二存储单元，用于存储所述临时文件；

[88] 第三发送单元，用于向所述信任中心发送存储所述临时文件对应的临时 URL；以便于所述信任中心将所述临时密钥和临时 URL 发送给第二用户；

[89] 第四接收单元，用于接收所述第二用户发送的获取所述临时 URL 对应的临时文件的请求；

[90] 第四发送单元，用于向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件。

[91] 由上述技方案可知，本发明实施例中，通过对用户数据（即共享文件）在上传到云端服务器之前进行加密，并且，通过信任中心对第一用户授权其他用户访问上传到云端的用户数据进行鉴权，解决了共享云端服务器上的共享文件的安全问题，提升了用户终端对于云安全的信心，并且用户可以方便的共享存储在云端服务器的共享数据。

附图说明

[92] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例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发明的一些实施例，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，还可以根据这些附图获得其他的附图。

[93] 图 1 为本发明实施例提供的一种数据共享的方法的流程图；

[94] 图 2 为本发明实施例提供的一种数据共享的方法的另一流程图；

[95] 图 3 为本发明实施例提供的一种数据共享的方法的又一流程图；

[96] 图 4 为本发明实施例提供的一种数据共享的方法的又一流程图；

[97] 图 5 为本发明实施例提供的一种数据共享的方法的又一流程图；

[98] 图 6 为本发明实施例提供的一种数据共享的方法的又一流程图；

[99] 图 7 为本发明实施例提供的一种数据共享装置的结构示意图；

[100] 图 8 为本发明实施例提供的一种数据共享装置的另一结构示意图；

[101] 图 9 为本发明实施例提供的一种数据共享装置的又一结构示意图；

[102] 图 10 为本发明实施例提供的一种数据共享装置的又一结构示意图；

[103] 图 11 为本发明实施例提供的一种数据共享装置的又一结构示意图；

[104] 图 12 为本发明实施例提供的一种数据共享装置的又一结构示意图；

[105] 图 13 为本发明实施例提供的一种数据共享的方法的第一应用实例图；

[106] 图 14 为本发明实施例提供的一种数据共享的方法的第二应用实例图；

[107] 图 15 为本发明实施例提供的一种数据共享的方法的第三应用实例图。

具体实施方式

[108] 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的描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的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。

[109] 请参阅图 1，图 1 为本发明实施例提供的一种数据共享的方法的流程图；在该实施例中，在用户终端（消费者）和云端服务器（云端服务提供商的服务器）之间引入了信任中心（即第三方），在该实施例中，假定云端服务提供商不可信。其中，信任中心包括证书授权中心(Certificate Authority, CA)和密钥分发中心(Key Distribution Center, KDC)，在该实施例中，通常默认用户终端和信任中心之间的通信信道是安全的，所以用户终端和信任中心之间的密钥协商过程也是安全的。所述方法包括：

[110] 步骤 101：接收第二用户通过统一资源定位符 URL 请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用所述第一用户的用户密钥加密后的共享文件；

[111] 在该步骤中，第一用户先使用自身的用户密钥对要上传的共享文件进行加密，得到加密后的共享文件，以及使用信任中心自身的公钥对所述用户密钥进行加密，并将加密后的用户密钥作为所述共享文件的文件描述，然后，第一用户将所述文件描述和加密后的共享文件上传到云端服务器上，并接收到所述云端服务器反馈的与所述共享文件对应的统一资源定位符（URL），之后，第一用户通过所述信任中心授权第二用户访问加密后所述共享文件的 URL，并通过信任中心验证所述第二用户为合法用户后，将所述 URL 发送给第二用户。

[112] 之后，信任中心就接收到所述第二用户请求获取所述 URL 对应的共享文件的用户密钥。

[113] 步骤 102：根据所述 URL 从云端服务器中获取所述共享文件的文件描述；其中，所述文件描述为利用信任中心的公钥加密所述用户密钥后的文件描述；

[114] 在该步骤 101 的基础上，信任中心向云端服务器请求获取所述 URL 对应的文件描述，以及接收到所述云端服务器反馈的所述文件描述。

[115] 步骤 103：利用信任中心的所述公钥对应的私钥解密所述文件描述，得到第一用户的用户密钥；

[116] 在该步骤中，由于信任中心在接收到所述 URL 对应的文件描述后，利用所述公钥对应的私钥对所述文件描述进行解密，得到第一用户的用户密钥。

[117] 步骤 104：将所述用户密钥发送给所述第二用户，以便于所述第二用户利用所述用户密钥解密获取到的所述共享文件，得到第一用户的原共享文件。

[118] 在该步骤中，信任中心可以通过安全通道将所述用户密钥发送给第二用户，第二用户先根据所述 URL 从云端服务器中获取到对应的共享文件，然后，再利用所述用户密钥对获取到的所述共享文件进行解密，得到第一用户的原共享文件。

[119] 本发明实施例中，通过对用户数据（即共享文件）在上传到云端服务器之前进行加密，并且，通过信任中心对第一用户授权其他用户访问上传到云端的用户数据进行鉴权，解决了共享云端服务器上的共享文件的安全问题，提升了用户终端对于云安全的信心，并且用户可以方便的共享存储在云端服务器的共享数据。

[120] 可选的，在另一实施例中，该实施例在上述实施例的基础上，还可以包括：信任中心在根据所述 URL 从云端服务器中获取所述共享文件的文件描述的同时，还获取与所述 URL 对应的所述共享文件；然后，利用所述用户密钥对获取到的所述共享文件进行解密，得到第一用户的原共享文件；之后，利用临时密钥加密所述第一用户的原共享文件，得到临时文件；以及将所述临时文件存储到所述云端服务器中，并获得所述云端服务器下发的与临时文件对应的临时 URL；

[121] 所述将用户密钥发送给所述第二用户，以便于所述第二用户利用所述用户密钥解密获取到的所述共享文件，得到第一用户的原共享文件具体为：将所述临时 URL 及临时密钥发送给所述第二用户，以便于所述第二用户利用所述临时密钥解密获取到的所述临时文件，得到第一用户的原共享文件。

[122] 也就是说，该实施例中，信任中心在获取到其他用户访问的共享文件和文件描述后，利用所述公钥对应的私钥对文件描述进行解密，得到对应的用户密钥，然后利用用户密钥对所述共享文件进行解密，得到原共享文件，然后，对所述原共享文件进行重新加密，以及将重新加密后的共享文件（即临时文件）重新上传到云端服务器，并得到云端服务器下发对应的临时 URL，然后，将其临时 URL 和临时密钥发送给第二用户，以便于第二

用户根据临时 URL 获取到对应的临时文件，以及利用临时密钥对所述临时文件进行解密，得到第一用户的原共享文件。

[123]本发明实施例中，信任中心对获取的原共享文件重新加密，并且重新上传到云端服务器上，以便于对第一用户授权其他用户访问上传到云端的用户数据进行鉴权，解决了共享云端服务器上的共享文件的安全问题，同时也方便用户共享存储在云端服务器的共享数据。

[124]还请参阅图 2，为本发明实施例提供的一种数据共享的方法的另一流程，所述方法包括：

[125]步骤 201：利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对用户密钥进行加密，并将加密后的用户密钥作为文件描述；

[126]在该步骤中，上传共享文件的用户（即第一用户）在上传共享文件前，先利用自身的密钥（即用户密钥）对共享文件进行加密，之后，利用信任中心的自身公钥对用户密钥进行加密，并将加密后的用户密钥作为该共享文件的文件描述。

[127]步骤 202：将所述共享文件和文件描述上传到所述云端服务器上；

[128]在该步骤中，第一用户通过安全通道将加密后的共享文件和文件描述上传云端服务器上，通常情况，默认用户和云端服务器之间是安全的。

[129]步骤 203：接收所述云端服务器发送的所述共享文件对应的统一资源定位符 URL，即 URL1；

[130]在该步骤中，第一用户通过安全通道接收所述云端服务器发送的与所述共享文件对应的 URL（即 URL1）。

[131]步骤 204：通过信任中心授权第二用户访问所述共享文件的 URL；

[132]第一用户通过信任中心先要对授权的第二用户的身份进行鉴权，即判断第二用户是否为合法用户，如果第二用户为合法用户，才会执行步骤 205；

[133]步骤 205：将所述 URL 发送给所述第二用户；以便于所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件，得到第一用户的原共享文件。

[134]在该步骤中，第二用户得到第一用户的原共享文件的过程主要包括两种情况：

[135]一种情况是，所述第二用户根据所述 URL 从所述信任中心获取所述共享文件的用户密钥，以及从云端服务器获取所述共享文件，并利用所述用户密钥解密所述共享文件，得到第一用户的原共享文件。

[136]另一种情况是，所述第二用户向信任中心请求所述 URL 对应的所述共享文件的用户密钥；所述第二用户接收所述信任中心响应所述请求发送的临时 URL 和临时密钥；其中，所述临时密钥是信任中心对获得的所述共享文件的原文件进行重新加密的密钥，所述临时 URL 是云端服务器返回临时文件对应的 URL，其中，所述临时文件为所述信任中心利用所述临时密钥对获得所述共享文件的原文件重新加密后的文件；所述第二用户向云端服务器获取所述临时 URL 对应的临时文件；并利用所述临时密钥对所述临时文件进行解密，得到所述第一用户的原共享文件。

[137]还请参阅图 3，为本发明实施例提供的一种数据共享的方法的又一流程图，其特征在于，包括：

[138]步骤 301：接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密所述用户密钥后的文件描述；

[139]云端服务器（或云端服务提供商的服务器）对接收到用户发送的共享文件及对应的文件描述进行存储，以及向用户反馈对应共享文件的统一资源定位符 URL，即步骤 302。

[140]步骤 302：存储所述共享文件及对应的文件描述；

[141]步骤 303：向所述第一用户发送存储所述共享文件对应的统一资源定位符 URL；

[142]云端服务器通过安全通道将所述共享文件的 URL 发送给对应的第一用户。之后，第一用户可以通过信任中心授权第二用户访问所述共享文件的 URL，在信任中心验证所述第二用户为合法用户时，第一用户将所述共享文件的 URL 发送给第二用户，之后，第二用户根据 URL 向信任中心请求所述共享文件的用户密钥，所述信任中心根据所述 URL 向云端服务器请求对应的文件描述。

[143]步骤 304：接收信任中心发送的获取所述 URL 对应的文件描述的请求；

[144]云端服务器通过安全信道接收信任中心发送的获取与所述 URL 对应的文件描述的请求。

[145]步骤 305：向所述信任中心发送包括所述文件描述的响应；以便于信任中心利用所述公钥对应的私钥解密所述文件描述，得到用户密钥，以及所述信任中心将所述用户密钥发送给第二用户；

[146]云端服务器通过安全信道向所述信任中心发送所述文件描述。

[147]步骤 306：接收第二用户发送请求所述 URL 对应的共享文件；所述第二用户为第一用户通过信任中心授权访问所述共享文件的用户；

[148]步骤 307：向所述第二用户发送所述 URL 对应的共享文件，以便于所述第二用户根据接收到的用户密钥解密所述共享文件，得到第一用户的原共享文件。

[149]还请参阅图 4，为本发明实施例提供的一种数据共享的方法的又一流程图，所述方法包括：

[150]步骤 401：接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

[151]云端服务器通过安全通道接收第一用户发送的共享文件及对应的文件描述。

[152]步骤 402：存储所述共享文件及对应的文件描述；

[153]步骤 403：向所述第一用户发送存储所述共享文件对应的统一资源定位符 URL；

[154]云端服务器通过安全通道将所述共享文件对应的 URL 发送给第一用户。

[155]步骤 404：接收信任中心发送的获取所述 URL 对应的共享文件和文件描述的请求；

[156]步骤 405：向所述信任中心发送包括所述共享文件和文件描述的响应；以便于信任中心利用所述公钥对应的私钥解密所述文件描述，得到用户密钥，并利用所述用户密钥解密所述共享文件，得到原文件；以及所述信任中心利用临时密钥对所述原文件进行加密，得到临时文件；

[157]也就是说，云端服务器，文件描述和共享文件发送给信任中心，信任中心根据所述公钥对应的私钥对文件描述进行解密，得到用户密钥，然后，利用用户密钥对共享文件进行解密，得到原共享文件，并且，在得到所述第一用户的原共享文件后，重新对该原共享文件进行加密，得到临时文件。

[158]步骤 406：接收所述信任中心发送的临时文件；

[159]步骤 407：向所述信任中心发送所述临时文件对应的临时 URL；以便于信任中心将所述临时密钥和临时 URL 发送给第二用户；

[160]其中，信任中心将重新加密后的临时文件上传到云端服务器上，得到云端服务器下发临时文件对应的临时 URL，之后，信任中心将所述临时密钥和临时 URL 发送给第二用户。

[161]步骤 408：接收所述第二用户发送的获取所述临时 URL 对应的临时文件的请求；

[162]步骤 409：向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件，得到原共享文件。

[163]还请参阅图 5，为本发明实施例提供的一种数据共享的方法的又一流程图，所述方法包括：

[164]步骤 501：接收信任中心发送的密钥，以及鉴权证书；

[165]第一用户接收到信任中心通过安全通道发送的密钥以及，对用户进行身份认证的鉴权证书。

[166]步骤 502：利用所述密钥对将要上传的共享文件进行加密，得到加密后的第一共享文件；

[167]第一用户利用密钥对要上传的共享文件进行加密，得到加密后的第一共享文件之后，执行步骤 503；

[168]步骤 503：将所述第一共享文件发送到云端服务器上；以便于所述云端服务器将所述第一共享文件作为第一用户的源文件；

[169]步骤 504：利用临时密钥对所述共享文件进行加密，得到加密后的第二共享文件；

[170]步骤 505：将所述第二共享文件发送到云端服务器上；以便于所述云端服务器将所述第二共享文件作为第一用户的临时文件；

[171]步骤 506：接收云端服务器发送的所述第二共享文件对应的统一资源定位符 URL；

[172]步骤 507：通过所述鉴权证书确认第二用户为合法用户后，将所述 URL 和临时密钥发送给第二用户；以便于所述第二用户请求所述 URL 对应的第二共享文件，并利用所述临时密钥解密所述第二共享文件，得到第一用户的原共享文件。

[173]还请参阅图 6，为本发明实施例提供的一种数据共享的方法的又一流程图，所述方法包括：

[174]步骤 601：接收第一用户发送的第一共享文件，所述第一共享文件为利用信任中心下发的密钥加密的文件；并将所述第一共享文件作为第一用户的源文件；

[175]步骤 602：接收所述第一用户发送的第二共享文件，所述第二共享文件为利用临时密钥加密的文件；并将所述第二共享文件作为所述第一用户的临时文件；

[176]步骤 603：存储第一共享文件和第二共享文件；

[177]在该步骤中，云端服务器可以将第一共享文件和第二共享文件存储到一个 URL，也可以存储在不同的 URL 下，本实施例不作限制。

[178]步骤 604：向所述第一用户发送存储所述第二共享文件对应的统一资源定位符 URL；

[179]步骤 605：接收第二用户发送获取所述 URL 对应的第二共享文件的请求，所述第二用户为所述第一用户经过鉴权认证的用户；并且接收到所述第一用户发送的临时密钥和所述 URL；

[180]步骤 606：向所述第二用户发送所述第二共享文件，以便于所述第二用户根据所述临时密钥解密所述第二共享文件，得到第一用户的原共享文件。

[181]基于上述方法的实现过程，本发明实施例还提供一种数据共享的装置，其结构示意图如图 7 所示，所述装置包括：第一接收单元 71，获取单元 72，第一解密单元 73 和第一发送单元 74，其中，所述第一接收单元 71，用于接收第二用户通过统一资源定位符 URL 请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述获取单元 72，用于根据所述 URL 从云端服务器中获取对应的所述共享文件的文件描述；其中，所述文件描述为利用信任中心的公钥加密所述用户密钥后的文件描述；所述第一解密单元 73，用于利用所述公钥对应的私钥解密所述文件描述，得到第一用户的用户密钥；所述第一发送单元 74，用于将所述用户密钥发送给所述第二用户，以便于所述第二用户利用所述用户密钥解密获取到的所述共享文件，得到第一用户的原共享文件。

[182]可选的，所述获取单元还可以用于：在根据所述 URL 从云端服务器中获取所述共享文件的文件描述的同时，还获取与所述 URL 对应的所述共享文件；所述装置还可以包括：第二解密单元，加密单元，第二发送单元和第二接收单元，其中，

[183]所述第二解密单元，用于利用所述第一解密单元得到的用户密钥解密获取的所述共享文件，得到第一用户的原共享文件；所述加密单元，用于利用临时密钥加密所述第一用户的原共享文件，得到临时文件；所述第二发送单元，用于将所述临时文件上传到所述云端服务器中；所述第二接收单元，用于接收所述云端服务器下发的与所述临时文件对应的临时 URL；所述第一发送单元，还用于将所述临时 URL 及临时密钥发送给所述第二用户，以便于所述第二用户利用所述临时密钥解密获取到的所述临时文件，得到第一用户的原共享文件。

[184]所述装置可以集成在信任中心中，也可以独立部署，本实施例不作限制。

[185]所述装置中各个单元的功能和作用的实现过程详见上述方法中对应的实现过程，在此不再赘述。

[186]还请参阅图 8，为本发明实施例提供的一种数据共享的装置的另一结构示意图，所述装置包括：加密单元 81，第一发送单元 82，第一接收单元 83，授权单元 84 和第二发送单元 85，其中，

[187]所述加密单元 81，用于利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对用户密钥进行加密，并将加密后的用户密钥作为文件描述；所述第一发送单元 82，用于将加密后的所述共享文件和文件描述上传到所述云端服务器上；所述第一接收单元 83，用于接收所述云端服务器发送的所述共享文件对应的统一资源定位符 URL；所述授权单元 84，用于通过信任中心授权第二用户访问所述共享文件的 URL；所述第二发送单元 85，用于将所述 URL 发送给所述第二用户；以便于所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件，得到第一用户的原共享文件。

[188]所述装置可以集成在用户终端中。

[189]所述装置中各个单元的功能和作用的实现过程详见上述方法中对应的实现过程，在此不再赘述。

[190]还请参阅图 9，为本发明实施例提供的一种数据共享的装置的又一结构示意图，所述装置包括：第一接收单元 91，存储单元 92，第一发送单元 93，第二接收单元 94，第二发送单元 95，第三接收单元 96 和第三发送单元 97，其中，

[191]所述第一接收单元 91，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；所述存储单元 92，用于存储所述共享文件及对

应的文件描述；所述第一发送单元 93，用于向所述第一用户发送存储所述共享文件对应的统一资源定位符 URL；所述第二接收单元 94，用于接收信任中心发送的获取所述 URL 对应的文件描述的请求；所述第二发送单元 95，用于向所述信任中心发送包括所述文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到用户密钥，以及所述信任中心将所述用户密钥发送给第二用户；所述第三接收单元 96，用于接收第二用户发送请求所述 URL 对应的共享文件；所述第二用户为第一用户通过信任中心授权访问所述共享文件的用户；所述第三发送单元 97，用于向所述第二用户发送所述 URL 对应的共享文件，以便于所述第二用户根据接收到的用户密钥解密所述共享文件，得到第一用户的原共享文件。

[192]所述装置可以集成在云端服务器中，也可以独立部署，本实施例不作限制。

[193]所述装置中各个单元的功能和作用的实现过程详见上述方法中对应的实现过程，在此不再赘述。

[194]还请参与图 10，为本发明实施例提供的一种数据共享的装置的又一结构示意图，所述装置包括：第一接收单元 11，第一存储单元 12，第一发送单元 13，第二接收单元 14，第二发送单元 15，第三接收单元 16，第二存储单元 17，第三发送单元 18，第四接收单元 19 和第四发送单元 120，其中，

[195]所述第一接收单元 11，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；所述第一存储单元 12，用于存储所述共享文件及对应的文件描述；所述第一发送单元 13，用于向所述第一用户发送存储所述共享文件和文件描述对应的统一资源定位符 URL；所述第二接收单元 14，用于接收信任中心发送的获取所述 URL 对应的共享文件和文件描述的请求；所述第二发送单元 15，用于向所述信任中心发送包括所述共享文件和文件描述的响应；以便于信任中心利用所述公钥对应的私钥解密所述文件描述，得到用户密钥，并利用所述用户密钥解密所述共享文件，得到原文件；以及所述信任中心利用临时密钥对所述原文件进行加密，得到临时文件；所述第三接收单元 16，用于接收所述信任中心发送的临时文件；所述第二存储单元 17，用于存储所述临时文件；所述第三发送单元 18，用于向所述信任中心发送存储所述临时文件对应的临时 URL；以便于信任中心将所述临时密钥和临时 URL 发送给第二用户；所述第四接收单元 19，用于接收所述第二用户发送的获取所述临时 URL 对应的临时文件的请求；所述第四发送单元 120，向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件，得到原共享文件。

[196]所述装置可以集成在云端服务器中，也可以独立部署，本实施例不作限制。

[197]所述装置中各个单元的功能和作用的实现过程详见上述方法中对应的实现过程，在此不再赘述。

[198]还请参阅图 11，为本发明实施例提供的一种数据共享的装置的又一结构示意图，所述装置包括：第一接收单元 111，第一加密单元 112，第一发送单元 113，第二加密单元 114，第二发送单元 115，第二接收单元 116 和第三发送单元 117，其中，

[199]所述第一接收单元 111，用于接收信任中心发送的密钥，以及鉴权证书；所述第一加密单元 112，用于利用所述密钥对将要上传的共享文件进行加密，得到加密后的第一共享文件；所述第一发送单元 113，用于将所述第一共享文件发送到云端服务器上；以便于所述云端服务器将所述第一共享文件作为第一用户的源文件；所述第二加密单元 114，用于利用临时密钥对所述共享文件进行加密，得到加密后的第二共享文件；所述第二发送单元 115，用于将所述第二共享文件发送到云端服务器上；以便于所述云端服务器将所述第二共享文件作为第一用户的临时文件；所述第二接收单元 116，用于接收云端服务器发送的所述第二共享文件对应的临时统一资源定位符 URL；所述第三发送单元 117，用于在通过所述鉴权证书确认第二用户为合法用户后，将所述临时 URL 和临时密钥发送给第二用户；以便于所述第二用户请求所述临时 URL 对应的第二共享文件，并利用所述临时密钥解密所述第二共享文件，得到第一用户的原共享文件。

[200]所述装置可以集成在用户终端。

[201]所述装置中各个单元的功能和作用的实现过程详见上述方法中对应的实现过程，在此不再赘述。

[202]还请参阅图 12，为本发明实施例提供的一种数据共享的装置的又一结构示意图，所述装置包括：第一接收单元 121，第二接收单元 122，存储单元 123，第一发送单元 124，第三接收单元 125 和第二发送单元 126，其中，

[203]所述第一接收单元 121，用于接收第一用户发送的第一共享文件，所述第一共享文件为利用信任中心下发的密钥加密的文件；并将所述第一共享文件作为第一用户的源文件；所述第二接收单元 122，用于接收所述第一用户发送的第二共享文件，所述第二共享文件为利用临时密钥加密的文件；并将所述第二共享文件作为所述第一用户的临时文件；所述存储单元 123，用于分别存储第一共享文件和第二共享文件；所述第一发送单元 124，用于向所述第一用户发送存储所述第二共享文件对应的临时统一资源定位符 URL；所述第三接收单元 125，用于接收第二用户发送的获取所述临时 URL 对应的第二共

享文件，所述第二用户为所述第一用户经过鉴权认证的用户；并且接收到所述第一用户发送的临时密钥和所述临时 URL；所述第二发送单元 126，用于向所述第二用户发送所述第二共享文件，以便于所述第二用户根据所述临时密钥解密所述第二共享文件，得到第一用户的原共享文件。

[204]所述装置可以集成在云端服务器上，也可以独立部署，本实施例不作限制。

[205]所述装置中各个单元的功能和作用的实现过程详见上述方法中对应的实现过程，在此不再赘述。

[206]为了便于本领域技术人员的理解，下面以具体的应用实例来说明。

[207]实施例一

[208]请参阅图 13，图 13 为本发明实施例提供的一种数据共享的方法的第一应用实例图，该实施例应用于在云环境下实现用户数据共享，所述方法包括：

[209]步骤 1301：用户 A 使用自己的用户密钥 key1 加密将要上传到云端服务器的共享文件，并使用信任中心的公钥加密用户密钥 key1 作为文件描述。

[210]其中，用户 A 使用信任中心的公钥，是通过第三方机构查询信任中心得到的。

[211]步骤 1302：用户 A 将已加密的所述共享文件和文件描述上传到云端服务器上。

[212]步骤 1303：云端服务器向用户 A 返回已上传共享文件所对应的统一资源定位符 URL。

[213]步骤 1304：用户 A 通过信任中心授权用户 B 访问该共享文件的 URL。

[214]步骤 1305：用户 A 发送云端服务器返回的共享文件的 URL 给用户 B。

[215]步骤 1306：信任中心对用户 B 进行身份鉴权，并在鉴权通过后，执行步骤 1307。

[216]也就是说，信任中心验证用户 B 是否为合法的用户，即对用户 B 的身份进行认证。

[217]步骤 1307：用户 B 通过所述 URL 向信任中心请求所述共享文件的用户密钥（即 key1）。即用户 B 向信任中心请求 URL 对应所述共享文件的用户密钥。

[218]步骤 1308：信任中心根据用户 B 请求中的 URL，向云端服务器请求其对应的文件描述。

[219]步骤 1309：云端服务器向信任中心返回所述 URL 对应的文件描述。

[220]步骤 1310：信任中心使用所述公钥对应的私钥（即与用户 A 使用的信任中心的公钥对应的私钥）解密文件描述，获得用户 A 的用户密钥 key1。

[221]步骤 1311：信任中心将用户 A 的用户密钥 key1 发送给用户 B，在该步骤中，可以通过信任中心与用户 B 之间的安全通道，也可以通过其他通道，本实施例中不作限制。

[222]步骤 1312：用户 B 向云端服务器请求所述 URL 对应的共享文件。

[223]步骤 1313：云端服务器向用户 B 返回所述 URL 对应的共享文件。

[224]步骤 1314：用户 B 使用接收到的所述用户 A 的用户密钥 key1 解密接收到的共享文件，获得用户 A 的原共享文件。

[225]本发明实施例中，通过对用户数据在上传到云端服务器之前进行加密操作，并且在信任中心授权的用户才可以访问上传到云端服务器上的数据，解决了共享云端文件的安全问题。提升了用户对于云安全的信心，并且使得用户可以方便的共享存储在云端的数据。

[226]实施例二

[227]请参阅图 14，图 14 为本发明实施例提供的一种数据共享的方法的第二应用实例图，该实施例应用于在云环境下实现用户数据共享，所述方法包括：

[228]步骤 1401：用户 A 使用自己的用户密钥 key1 加密将要上传到云端服务器的共享文件，并使用信任中心的公钥加密用户密钥 key1 作为文件描述。

[229]步骤 1402：用户 A 将已加密的共享文件和文件描述上传到云端服务器。

[230]步骤 1403：云端服务器向用户 A 返回已上传的共享文件所对应的 URL，为了便于描述，本实施例定义为 URL1。

[231]步骤 1404：用户 A 通过信任中心授权用户 B 访问该共享文件的 URL1。

[232]步骤 1405：用户 A 向用户 B 发送所述共享文件的 URL1。

[233]步骤 1406：信任中心对用户 B 进行身份鉴权，并在鉴权通过后，执行步骤 1407；

[234]其中，用户 B 通过信任中心实现身份认证。

[235]步骤 1407：用户 B 通过所述 URL1 向信任中心请求所述共享文件的用户密钥（即 key1）。

[236]步骤 1408：信任中心根据用户 B 请求中的 URL1，向云端服务器请求用户 A 上传的共享文件和文件描述。

[237]步骤 1409：云端服务器向所述信任中心返回用户 A 上传的共享文件和文件描述。

[238]步骤 1410：信任中心使用所述公钥对应的私钥对所述文件描述进行解密，获得用户 A 的用户密钥 key1，并使用 key1 解密所述共享文件，获得用户 A 的原共享文件；

[239]步骤 1411：信任中心使用临时密钥 key2 加密原共享文件，得到临时文件 file2。

[240]步骤 1412：信任中心将所述临时文件 file2 上传到云端服务器。

[241]步骤 1413：云端服务器向信任中心返回临时文件 file2 对应的临时 URL，为了便于描述，本实施例定义 URL2。

[242]步骤 1414：信任中心通过安全信道向用户 B 发送所述 URL2 和临时密钥 key2。

[243]步骤 1415：用户 B 向云端服务器请求所述 URL2 对应的临时文件 file2。

[244]步骤 1416：云端服务器向用户 B 返回所述 URL2 对应的临时文件 file2。

[245]步骤 1417：用户 B 接收所述临时文件 file2，并使用信任中心返回的临时密钥 key2 解密接收到的临时文件 file2，获得用户 A 的原共享文件。

[246]本发明实施例中，通过对用户数据在上传到云端服务器之前进行加密操作，并且在信任中心在获取到原共享文件后，对该原共享文件进行重新加密，以及将重新加密后的共享文件上传到云端服务器，以便于授权的用户访问上传到云端服务器上的数据，解决了共享云端文件的安全问题。提升了用户对于云安全的信心，并且使得用户可以方便的共享存储在云端的数据。

[247]实施例三

[248]请参阅图 15，图 15 为本发明实施例提供的一种数据共享的方法的第三应用实例图，该实施例应用于在云环境下实现用户数据共享，所述方法包括：

[249]步骤 1501：信任中心向用户 A 分发密钥 key1。

[250]其中，可以通过安全信道向用户 A 分发密钥 key1。

[251]步骤 1502：用户 A 使用所述密钥 key1 加密将要上传到云端服务器上的文件，得到加密后的文件 file1。

[252]步骤 1503：用户 A 将已加密的文件 file1 上传到云端服务器上。

[253]步骤 1504：云端服务器存储接收到的文件 file1，并将文件 file1 作为用户 A 的源文件。

[254]步骤 1505：用户 A 随机选择临时密钥 key2，并使用临时密钥 key2 加密所述文件，获得文件 file2。

[255]其中，步骤 1504 和步骤 1505 在时间上不分先后顺序，也可以同时进行。

[256]步骤 1506：用户 A 将已加密的文件 file2 上传到云端服务器上。

[257]步骤 1507：云端服务器存储接收到的文件 file2，并将文件 file2 作为用户 A 的临时文件，即称为临时文件 file2。

[258]步骤 1508：云端服务器向用户 A 发送所述临时文件 file2 对应的临时 URL；

[259]步骤 1509：用户 A 通过信任中心颁发的鉴权证书对用户 B 进行鉴权（认证），并在确认对方为合法用户后，执行步骤 1510；

[260]其中，步骤 1508 和步骤 1509 在时间上没有先后顺序，也可以同时进行，本实施例不作限制。

[261]步骤 1510：用户 A 将所述临时 URL 和临时密钥 key2 发送给用户 B。

[262]步骤 1511：用户 B 向云端服务器请求临时 URL 对应的临时文件 file2。

[263]步骤 1512：云端服务器向用户 B 返回所述临时 URL 对应的临时文件 file2。

[264]步骤 1513：用户 B 接收到临时文件 file2，并使用临时密钥 key2 解密所述临时文件 file2，获得用户 A 的原共享文件。

[265]本发明实施例，用户预先接收到信任中心的密钥，并通过该密钥对要共享的文件进行加密，得到 file1，并将 file1 上传到云端服务器，云端服务器会将该文件作为该用户的源文件，之后，该用户会用临时密钥对要共享的该文件进行加密，得到 file2，并将 file2 也上传到云端服务器，云端服务器会将该 file2 作为临时文件，并将该临时文件作为其他授权用户访问的文件，解决了共享云端文件的安全问题，同时也方便授权用户共享存储在云端服务器上的数据。

[266]本发明实施例还提供一种信任中心，所述信任中心包括：收发器和处理器，其中，

[267]所述收发器，用于接收第二用户通过统一资源定位符 URL 请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用所述用户密钥加密后的共享文件；以及根据所述 URL 从云端服务器中获取对应的所述共享文件的文件描述；其中，所述文件描述为利用所述信任中心的公钥加密所述用户密钥后的文件描述；

[268]所述处理器，利用所述信任中心的所述公钥对应的私钥解密所述文件描述，得到所述第一用户的所述用户密钥；

[269]所述收发器，还用于将所述用户密钥发送给所述第二用户。

[270]可选的，在另一实施例中，该实施例在上述实施例中，所述收发器根据所述 URL 从云端服务器中获取所述共享文件的文件描述，还包括：获取与所述 URL 对应的所述共享文件；

[271]所述处理器，还用于利用所述用户密钥解密获取的所述共享文件，得到所述第一用户的原共享文件；以及利用临时密钥加密所述原共享文件，得到临时文件；

[272]所述收发器，还用于将所述临时文件上传到所述云端服务器中，并获得所述云端服务器下发的与所述临时文件对应的临时 URL；

[273]所述收发器将用户密钥发送给所述第二用户，具体包括：将所述临时 URL 及临时密钥发送给所述第二用户。

[274]其中，所述信任中心包括的收发器和处理器的功能和作用的实现过程，详见上述方法中对应的实现过程，在此不再赘述。

[275]本发明实施例还提提供一种用户终端，包括：收发器和处理器，其中，

[276]所述处理器，用于利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对所述用户密钥进行加密，并将加密后的用户密钥作为文件描述；

[277]所述收发器，用于将加密后的所述共享文件和文件描述上传到所述云端服务器；以及接收所述云端服务器发送的所述共享文件对应的统一资源定位符 URL；

[278]所述处理器，用于通过所述信任中心授权第二用户访问所述共享文件；

[279]所述收发器，还用于将所述 URL 发送给所述第二用户；以便于所述第二用户根据所

述 URL 获取所述用户密钥；并利用所述用户密钥解密所述共享文件。

[280]其中，所述用户终端包括的收发器和处理器的功能和作用的实现过程，详见上述方法中对应的实现过程，在此不再赘述。

[281]本发明实施例还提供一种云端服务器，包括：收发器和存储器，其中，

[282]所述收发器，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

[283]所述存储器，用于存储所述共享文件及对应的文件描述；

[284]所述收发器，还用于向所述第一用户发送存储所述共享文件对应的统一资源定位符 URL；接收信任中心发送的获取所述 URL 对应的文件描述的请求；向所述信任中心发送包括所述文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，以及所述信任中心将所述用户密钥发送给第二用户；接收第二用户发送请求所述 URL 对应的共享文件；所述第二用户为所述第一用户通过所述信任中心授权访问所述共享文件的用户；向所述第二用户发送所述 URL 对应的共享文件，以便于所述第二用户根据接收到的所述用户密钥解密所述共享文件。

[285]其中，所述云端服务器包括的收发器和存储器的功能和作用的实现过程，详见上述方法中对应的实现过程，在此不再赘述。

[286]本发明实施例还提供一种云端服务器，包括：收发器和存储器，其中，

[287]所述收发器，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

[288]所述存储器，用于存储所述共享文件及对应的文件描述；

[289]所述收发器，还用于向所述第一用户发送存储所述共享文件和对应的文件描述对应的统一资源定位符 URL；接收信任中心发送的获取所述 URL 对应的共享文件和文件描述的请求；向所述信任中心发送包括所述共享文件和文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，并利用所述用户密钥解密所述共享文件后利用临时密钥重新加密，得到临时文件；接收所述信任中心发送的临时文件；

[290]所述存储器，还用于存储所述临时文件；

[291]所述收发器，还用于向所述信任中心发送存储所述临时文件对应的临时 URL；以便于所述信任中心将所述临时密钥和临时 URL 发送给第二用户；接收所述第二用户发送的获取所述临时 URL 对应的临时文件的请求；向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件。

[292]其中，所述云端服务器包括的收发器和存储器的功能和作用的实现过程，详见上述方法中对应的实现过程，在此不再赘述。

[293]需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[294]通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[295]以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权 利 要 求

1、一种数据共享的方法，其特征在于，包括：

接收第二用户通过统一资源定位符 URL 请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用所述用户密钥加密后的共享文件；

根据所述 URL 从云端服务器中获取对应的所述共享文件的文件描述；其中，所述文件描述为利用所述信任中心的公钥加密所述用户密钥后的文件描述；

利用所述信任中心的所述公钥对应的私钥解密所述文件描述，得到所述第一用户的所述用户密钥；

将所述用户密钥发送给所述第二用户。

2、根据权利要求 1 所述的方法，其特征在于，所述根据所述 URL 从云端服务器中获取所述共享文件的文件描述，还包括：

获取与所述 URL 对应的所述共享文件；

利用所述用户密钥解密获取的所述共享文件，得到所述第一用户的原共享文件；

利用临时密钥加密所述原共享文件，得到临时文件；

将所述临时文件上传到所述云端服务器中，并获得所述云端服务器下发的与所述临时文件对应的临时 URL；

所述将用户密钥发送给所述第二用户，具体包括：

将所述临时 URL 及临时密钥发送给所述第二用户。

3、一种数据共享的方法，其特征在于，包括：

利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对所述用户密钥进行加密，并将加密后的用户密钥作为文件描述；

将加密后的所述共享文件和文件描述上传到所述云端服务器；

接收所述云端服务器发送的所述共享文件对应的统一资源定位符 URL；

通过所述信任中心授权第二用户访问所述共享文件；

将所述 URL 发送给所述第二用户；以便于所述第二用户根据所述 URL 获取所述用户密钥；并利用所述用户密钥解密所述共享文件。

4、根据权利要求 3 所述的方法，其特征在于，所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件，具体包括：

所述第二用户根据所述 URL 从所述信任中心获取所述共享文件的所述用户密钥，以及从所述云端服务器获取所述共享文件，并利用所述用户密钥解密所述共享文件。

5、根据权利要求 3 所述的方法，其特征在于，所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件，具体包括：

所述第二用户向所述信任中心请求所述 URL 对应的所述共享文件的所述用户密钥；

接收所述信任中心响应所述请求发送的临时 URL 和临时密钥；其中，所述临时密钥是信任中心对获得的所述共享文件解密后进行重新加密的密钥，所述临时 URL 是云端服务器返回临时文件对应的 URL，其中，所述临时文件为所述信任中心利用所述临时密钥对获得所述共享文件解密后重新加密后的文件；

向云端服务器获取所述临时 URL 对应的临时文件；

利用所述临时密钥对所述临时文件进行解密。

6、一种数据共享的方法，其特征在于，包括：

接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

存储所述共享文件及对应的文件描述；

向所述第一用户发送存储所述共享文件对应的统一资源定位符 URL；

接收信任中心发送的获取所述 URL 对应的文件描述的请求；

向所述信任中心发送包括所述文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，以及所述信任中心将所述用户密钥发送给第二用户；

接收第二用户发送请求所述 URL 对应的共享文件；所述第二用户为所述第一用户通过所述信任中心授权访问所述共享文件的用户；

向所述第二用户发送所述 URL 对应的共享文件，以便于所述第二用户根据接收到的所述用户密钥解密所述共享文件。

7、一种数据共享的方法，其特征在于，包括：

接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

存储所述共享文件及对应的文件描述；

向所述第一用户发送存储所述共享文件和对应的文件描述对应的统一资源定位符 URL；

接收信任中心发送的获取所述 URL 对应的共享文件和文件描述的请求；

向所述信任中心发送包括所述共享文件和文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，并利用所述用户密钥解密所述共享文件后利用临时密钥重新加密，得到临时文件；

接收所述信任中心发送的临时文件；

存储所述临时文件；

向所述信任中心发送存储所述临时文件对应的临时 URL；以便于所述信任中心将所述临时密钥和临时 URL 发送给第二用户；

接收所述第二用户发送的获取所述临时 URL 对应的临时文件的请求；

向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件。

8、一种数据共享的装置，其特征在于，包括：

第一接收单元，用于接收第二用户通过统一资源定位符 URL 请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用所述第一用户的用户密钥加密后的共享文件；

获取单元，用于根据所述 URL 从云端服务器中获取对应的所述共享文件的文件描述；其中，所述文件描述为利用所述信任中心的公钥加密所述用户密钥后的文件描述；

第一解密单元，用于利用所述信任中心的所述公钥对应的私钥解密所述文件描述，得到所述第一用户的用户密钥；

第一发送单元，用于将所述用户密钥发送给所述第二用户。

9、根据权利要求 8 所述的装置，其特征在于，所述获取单元还用于：在根据所述 URL 从云端服务器中获取所述共享文件的文件描述时，还获取与所述 URL 对应的所述共享文件；所述装置还包括：

第二解密单元，用于利用所述第一解密单元得到的所述用户密钥解密获取的所述共享文件，得到第一用户的原共享文件；

加密单元，用于利用临时密钥加密所述原共享文件，得到临时文件；

第二发送单元，用于将所述临时文件上传到所述云端服务器中；

第二接收单元，用于所述云端服务器下发的与所述临时文件对应的临时 URL；

所述第一发送单元，还用于将所述临时 URL 及临时密钥发送给所述第二用户。

10、一种数据共享的装置，其特征在于，包括：

加密单元，用于利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对所述用户密钥进行加密，并将加密后的用户密钥

作为文件描述；

第一发送单元，用于将加密后的所述共享文件和文件描述上传到所述云端服务器；

第一接收单元，用于接收所述云端服务器发送的所述共享文件对应的统一资源定位符 URL；

授权单元，用于通过所述信任中心授权第二用户访问所述共享文件；

第二发送单元，用于将所述 URL 发送给所述第二用户；以便于所述第二用户根据所述 URL 获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件。

11、一种数据共享的装置，其特征在于，包括：

第一接收单元，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

存储单元，用于存储所述共享文件及对应的文件描述；

第一发送单元，用于向所述第一用户发送存储所述共享文件对应的统一资源定位符 URL；

第二接收单元，用于接收信任中心发送的获取所述 URL 对应的文件描述的请求；

第二发送单元，用于向所述信任中心发送包括所述文件描述的响应；以便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，以及所述信任中心将所述用户密钥发送给第二用户；

第三接收单元，用于接收第二用户发送请求所述 URL 对应的共享文件；所述第二用户为所述第一用户通过所述信任中心授权访问所述共享文件的用户；

第三发送单元，用于向所述第二用户发送所述 URL 对应的共享文件，以便于所述第二用户根据接收到的所述用户密钥解密所述共享文件。

12、一种数据共享的装置，其特征在于，包括：

第一接收单元，用于接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述；

第一存储单元，用于存储所述共享文件及对应的文件描述；

第一发送单元，用于向所述第一用户发送存储所述共享文件和文件描述对应的统一资源定位符 URL；

第二接收单元，用于接收信任中心发送的获取所述 URL 对应的共享文件和文件描述的请求；

第二发送单元，用于向所述信任中心发送包括所述共享文件和文件描述的响应；以

便于所述信任中心利用所述公钥对应的私钥解密所述文件描述，得到所述用户密钥，并利用所述用户密钥解密所述共享文件后利用临时密钥重新加密，得到临时文件；

第三接收单元，用于接收所述信任中心发送的临时文件；

第二存储单元，用于存储所述临时文件；

第三发送单元，用于向所述信任中心发送存储所述临时文件对应的临时 URL；以便于所述信任中心将所述临时密钥和临时 URL 发送给第二用户；

第四接收单元，用于接收所述第二用户发送的获取所述临时 URL 对应的临时文件的请求；

第四发送单元，用于向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件。

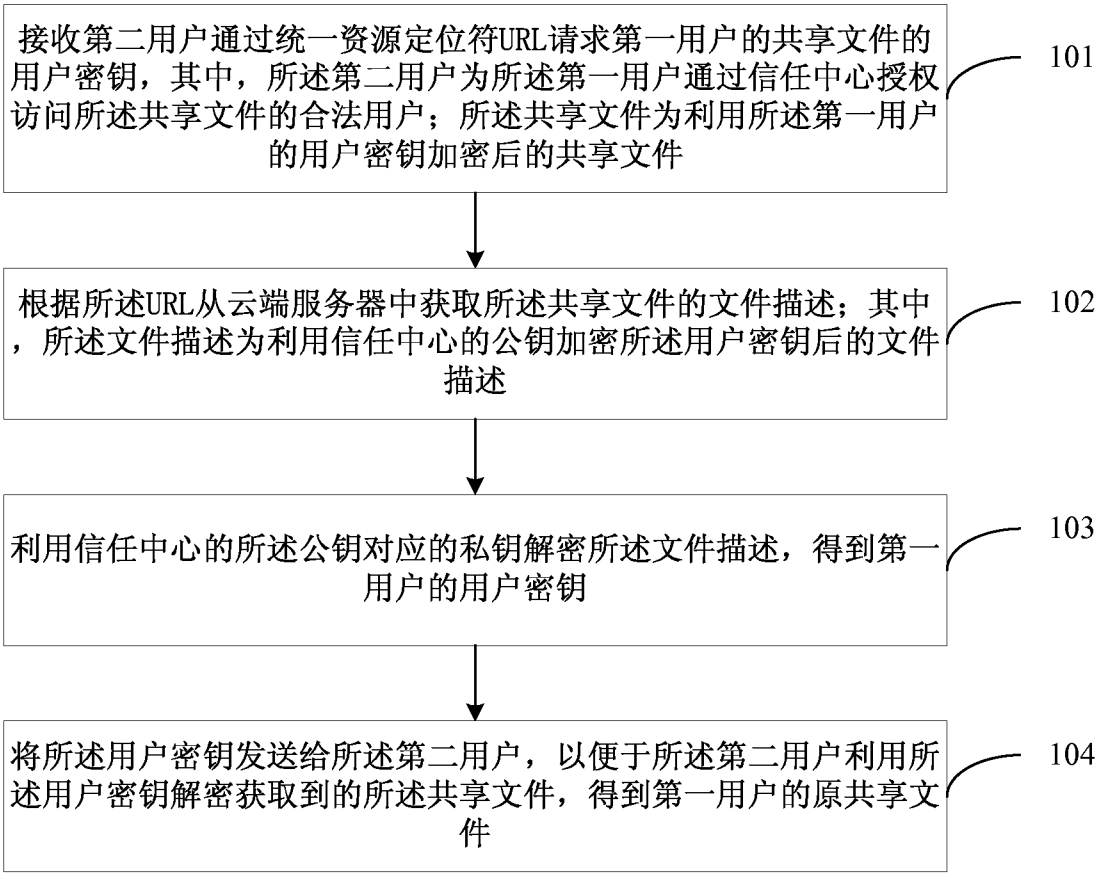
接收第二用户通过统一资源定位符URL请求第一用户的共享文件的用户密钥，其中，所述第二用户为所述第一用户通过信任中心授权访问所述共享文件的合法用户；所述共享文件为利用所述第一用户的用户密钥加密后的共享文件
101
根据所述URL从云端服务器中获取所述共享文件的文件描述；其中，所述文件描述为利用信任中心的公钥加密所述用户密钥后的文件描述
102
利用信任中心的所述公钥对应的私钥解密所述文件描述，得到第一用户的用户密钥
103
将所述用户密钥发送给所述第二用户，以便于所述第二用户利用所述用户密钥解密获取到的所述共享文件，得到第一用户的原共享文件
104

图 1

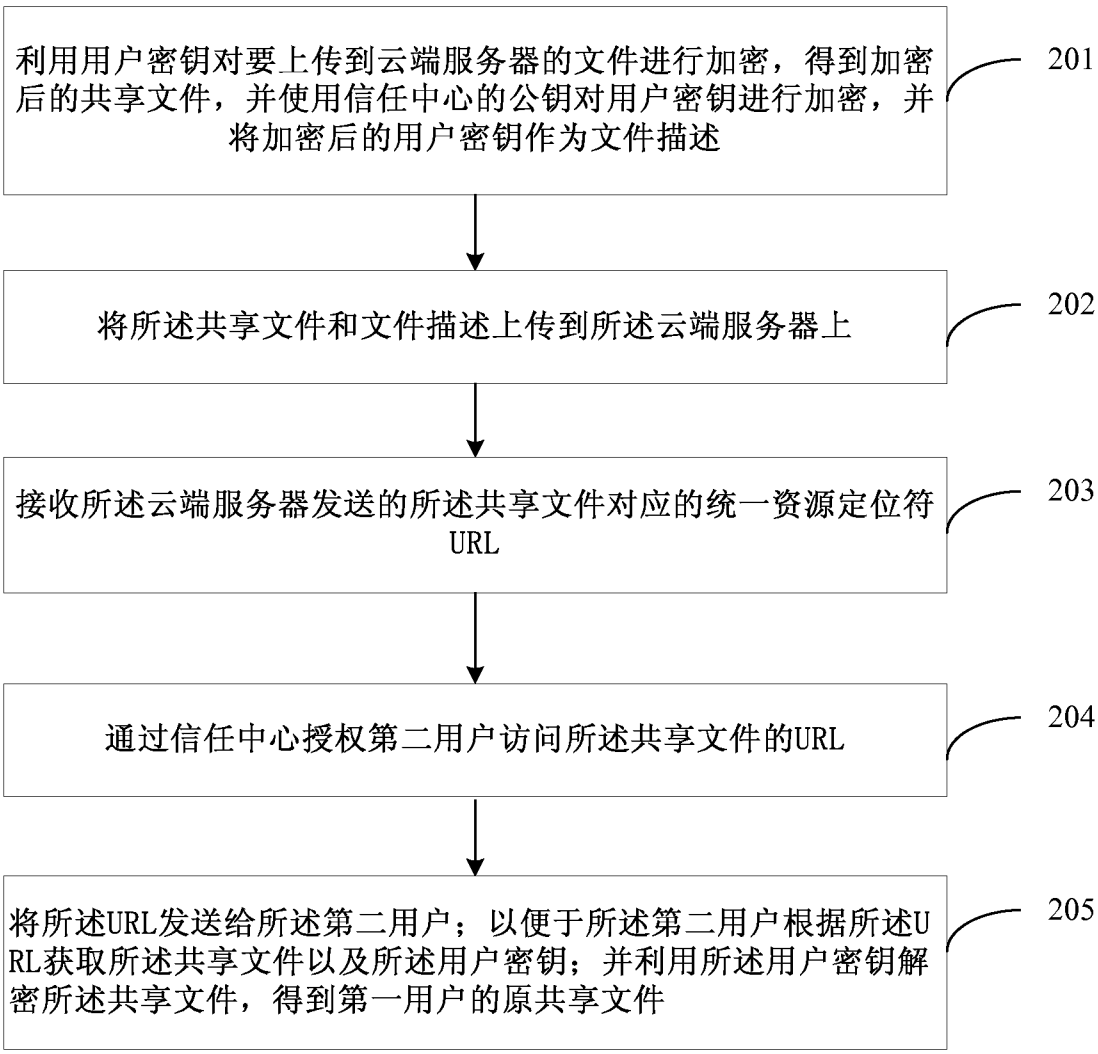
利用用户密钥对要上传到云端服务器的文件进行加密，得到加密后的共享文件，并使用信任中心的公钥对用户密钥进行加密，并将加密后的用户密钥作为文件描述
201
将所述共享文件和文件描述上传到所述云端服务器上
202
接收所述云端服务器发送的所述共享文件对应的统一资源定位符URL
203
通过信任中心授权第二用户访问所述共享文件的URL
204
将所述URL发送给所述第二用户；以便于所述第二用户根据所述URL获取所述共享文件以及所述用户密钥；并利用所述用户密钥解密所述共享文件，得到第一用户的原共享文件
205

图 2

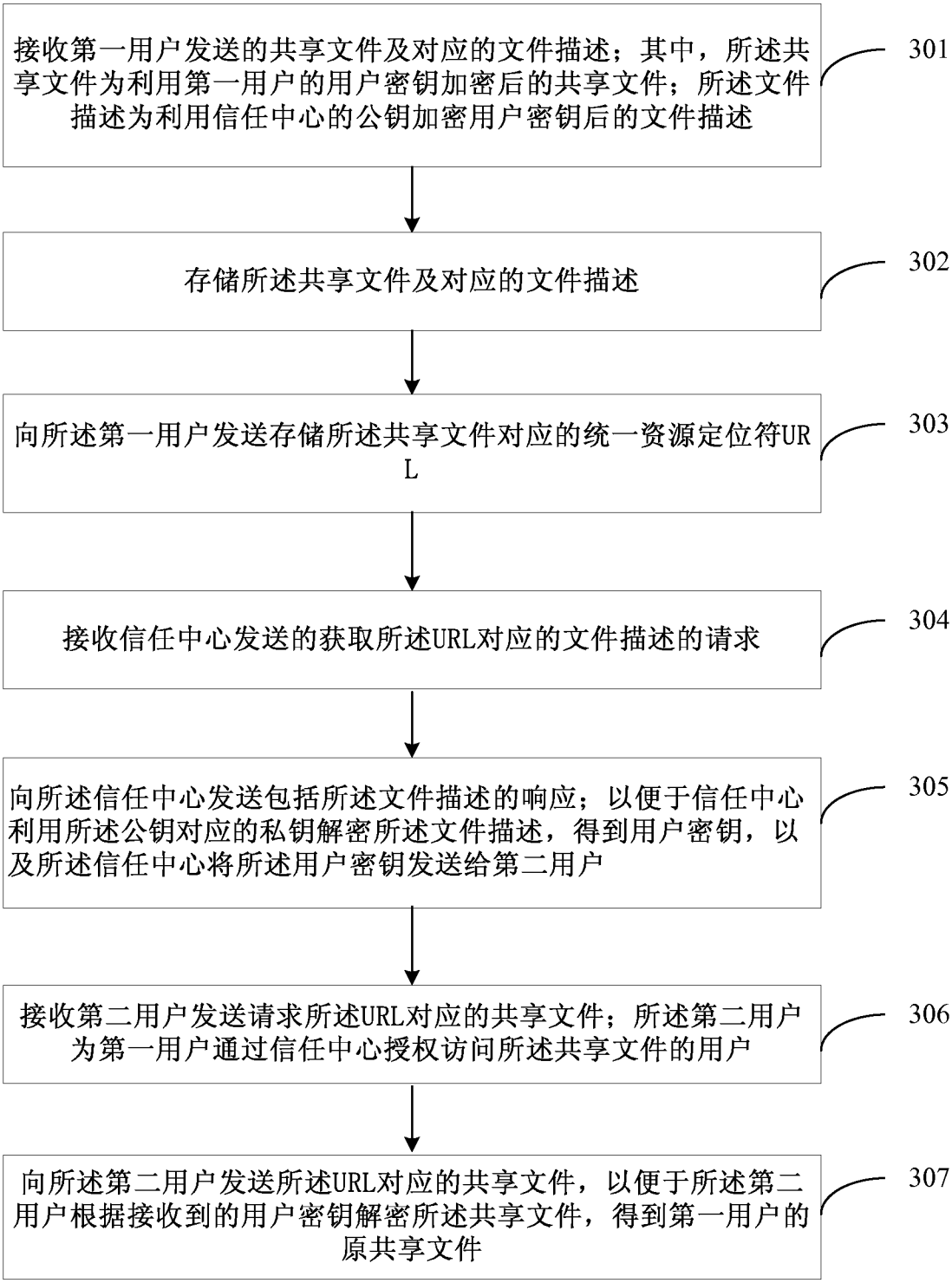
接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述
301
存储所述共享文件及对应的文件描述
302
向所述第一用户发送存储所述共享文件对应的统一资源定位符URL
303
接收信任中心发送的获取所述URL对应的文件描述的请求
304
向所述信任中心发送包括所述文件描述的响应；以便于信任中心利用所述公钥对应的私钥解密所述文件描述，得到用户密钥，以及所述信任中心将所述用户密钥发送给第二用户
305
接收第二用户发送请求所述URL对应的共享文件；所述第二用户为第一用户通过信任中心授权访问所述共享文件的用户
306
向所述第二用户发送所述URL对应的共享文件，以便于所述第二用户根据接收到的用户密钥解密所述共享文件，得到第一用户的原共享文件
307

图 3

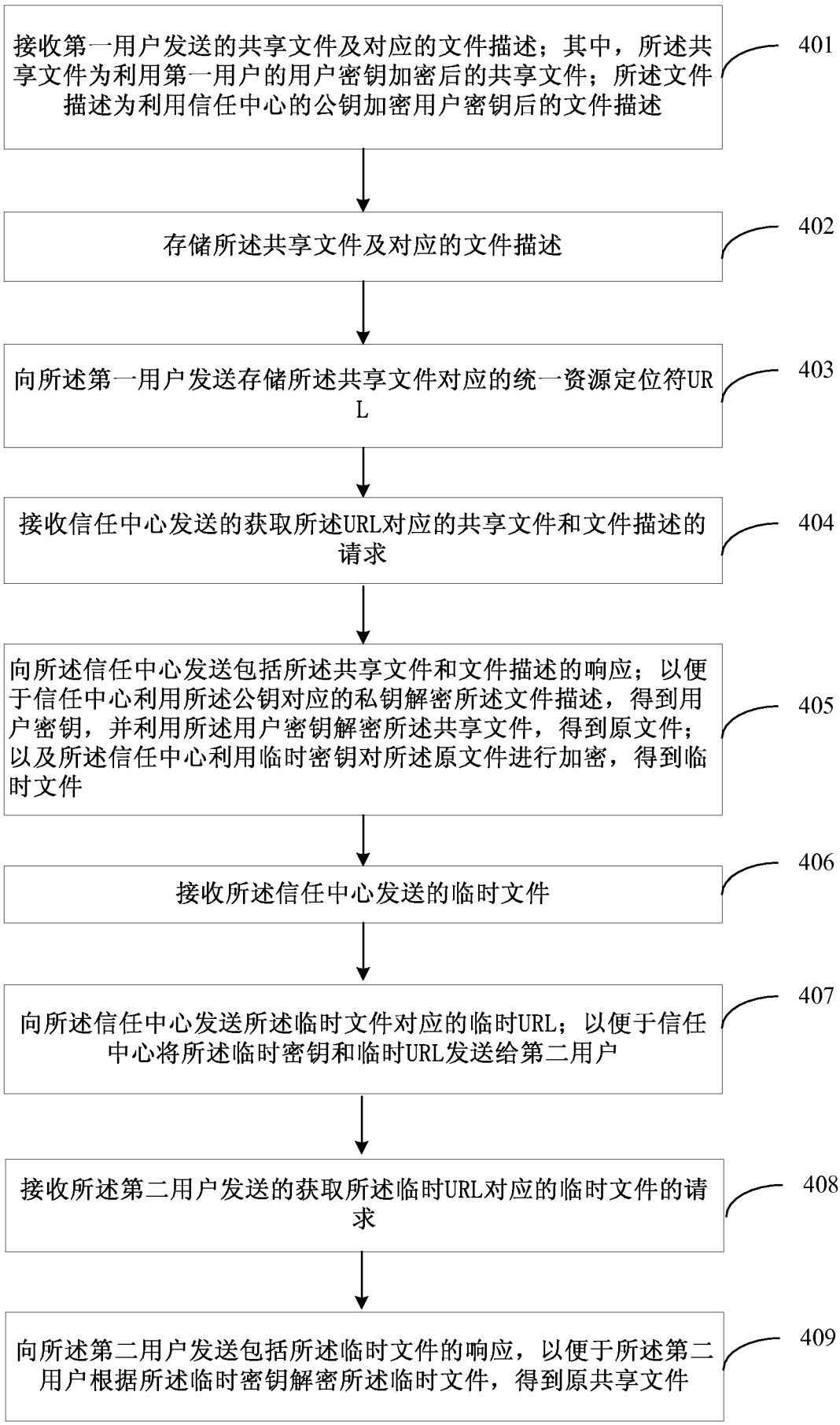
接收第一用户发送的共享文件及对应的文件描述；其中，所述共享文件为利用第一用户的用户密钥加密后的共享文件；所述文件描述为利用信任中心的公钥加密用户密钥后的文件描述
401
存储所述共享文件及对应的文件描述
402
向所述第一用户发送存储所述共享文件对应的统一资源定位符URL
403
接收信任中心发送的获取所述URL对应的共享文件和文件描述的请求
404
向所述信任中心发送包括所述共享文件和文件描述的响应；以便于信任中心利用所述公钥对应的私钥解密所述文件描述，得到用户密钥，并利用所述用户密钥解密所述共享文件，得到原文件；以及所述信任中心利用临时密钥对所述原文件进行加密，得到临时文件
405
接收所述信任中心发送的临时文件
406
向所述信任中心发送所述临时文件对应的临时URL；以便于信任中心将所述临时密钥和临时URL发送给第二用户
407
接收所述第二用户发送的获取所述临时URL对应的临时文件的请求
408
向所述第二用户发送包括所述临时文件的响应，以便于所述第二用户根据所述临时密钥解密所述临时文件，得到原共享文件
409

图 4

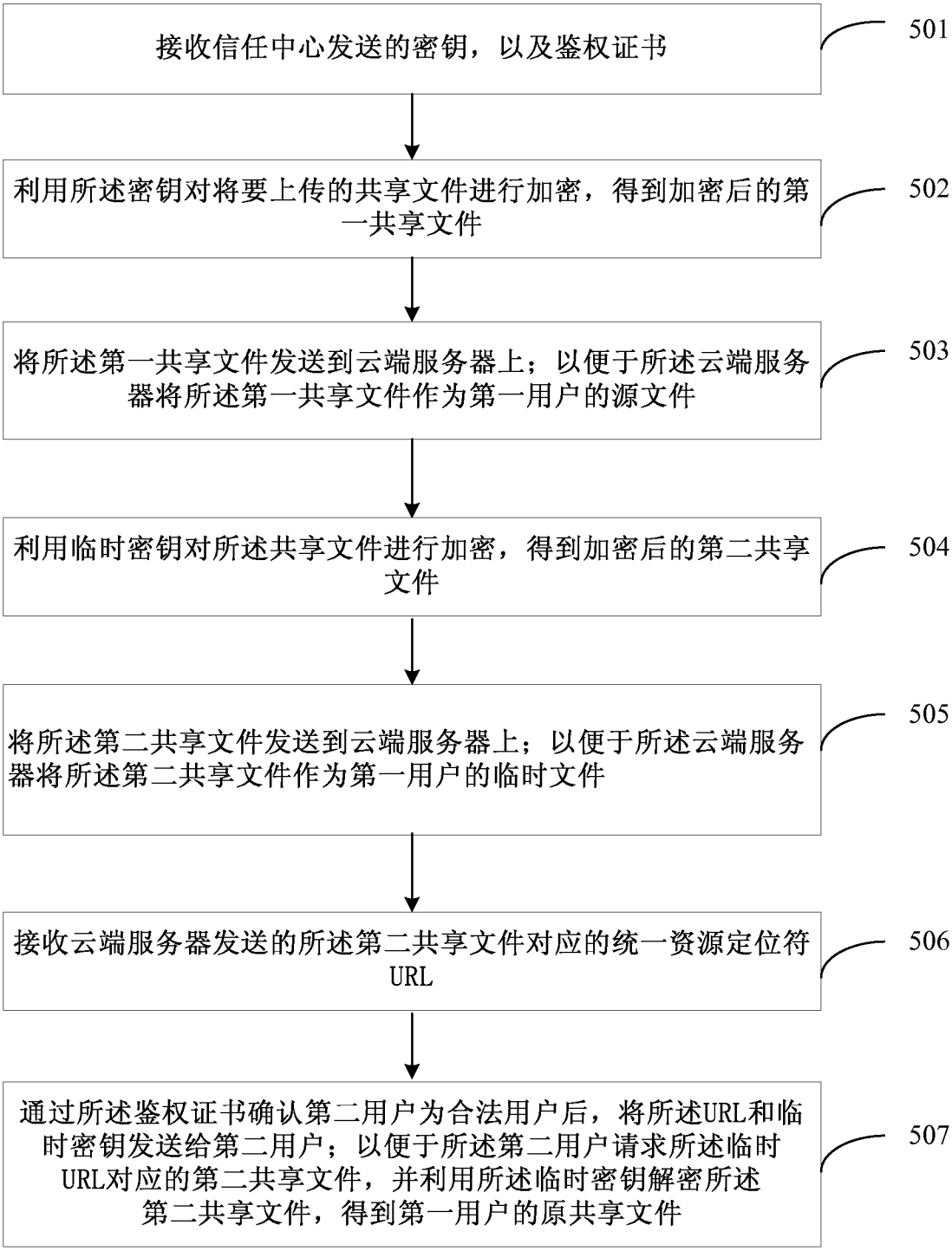
接收信任中心发送的密钥，以及鉴权证书
501
利用所述密钥对将要上传的共享文件进行加密，得到加密后的第一共享文件
502
将所述第一共享文件发送到云端服务器上；以便于所述云端服务器将所述第一共享文件作为第一用户的源文件
503
利用临时密钥对所述共享文件进行加密，得到加密后的第二共享文件
504
将所述第二共享文件发送到云端服务器上；以便于所述云端服务器将所述第二共享文件作为第一用户的临时文件
505
接收云端服务器发送的所述第二共享文件对应的统一资源定位符URL
506
通过所述鉴权证书确认第二用户为合法用户后，将所述URL和临时密钥发送给第二用户；以便于所述第二用户请求所述临时URL对应的第二共享文件，并利用所述临时密钥解密所述第二共享文件，得到第一用户的原共享文件
507

图 5

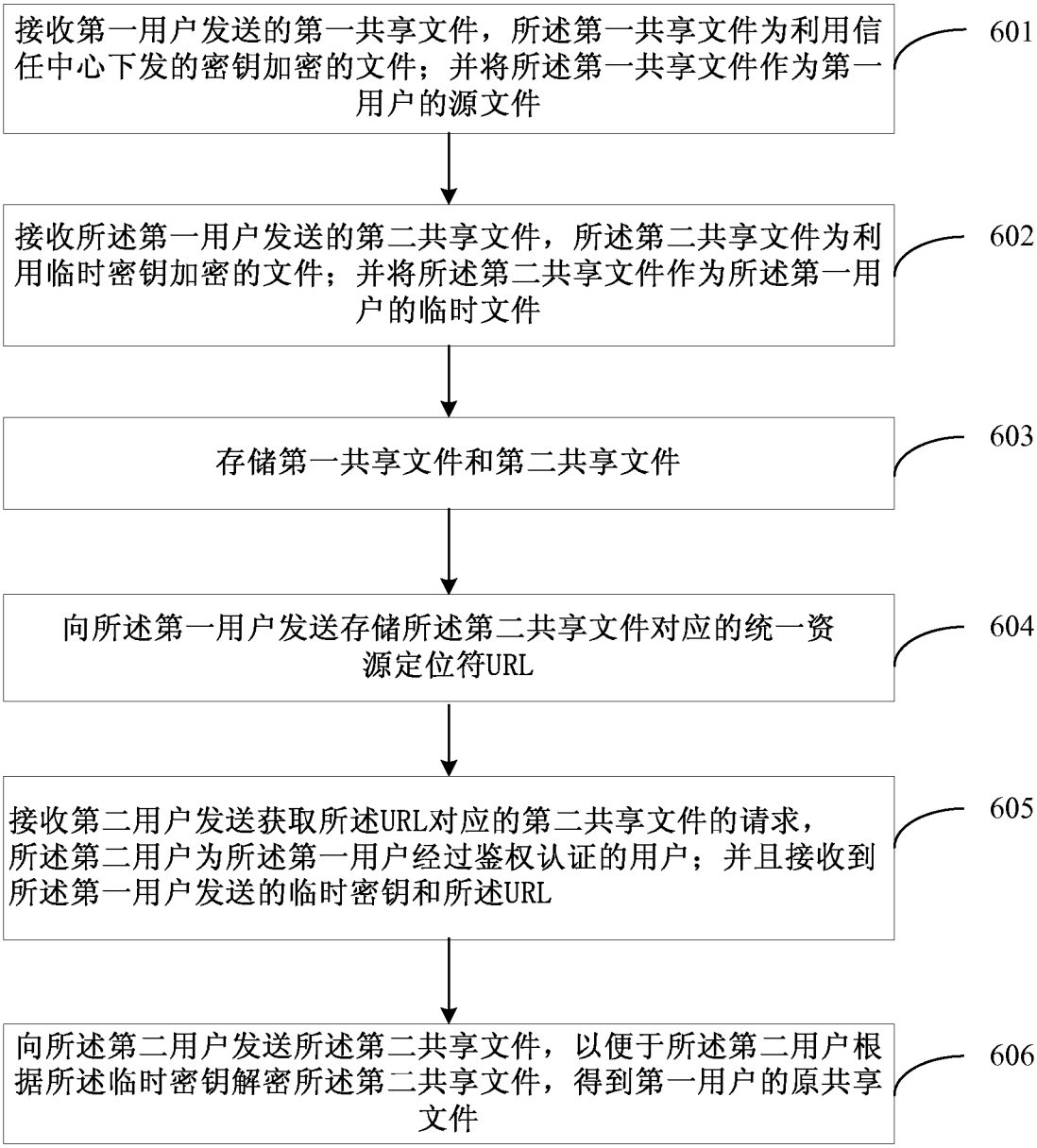
接收第一用户发送的第一共享文件，所述第一共享文件为利用信任中心下发的密钥加密的文件；并将所述第一共享文件作为第一用户的源文件
601
接收所述第一用户发送的第二共享文件，所述第二共享文件为利用临时密钥加密的文件；并将所述第二共享文件作为所述第一用户的临时文件
602
存储第一共享文件和第二共享文件
603
向所述第一用户发送存储所述第二共享文件对应的统一资源定位符URL
604
接收第二用户发送获取所述URL对应的第二共享文件的请求，所述第二用户为所述第一用户经过鉴权认证的用户；并且接收到所述第一用户发送的临时密钥和所述URL
605
向所述第二用户发送所述第二共享文件，以便于所述第二用户根据所述临时密钥解密所述第二共享文件，得到第一用户的原共享文件
606

图 6

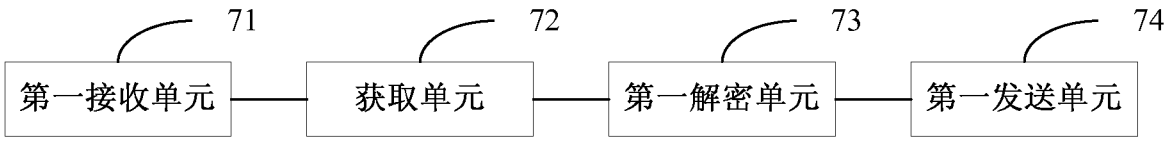
71
第一接收单元
72
获取单元
73
第一解密单元
74
第一发送单元

图 7

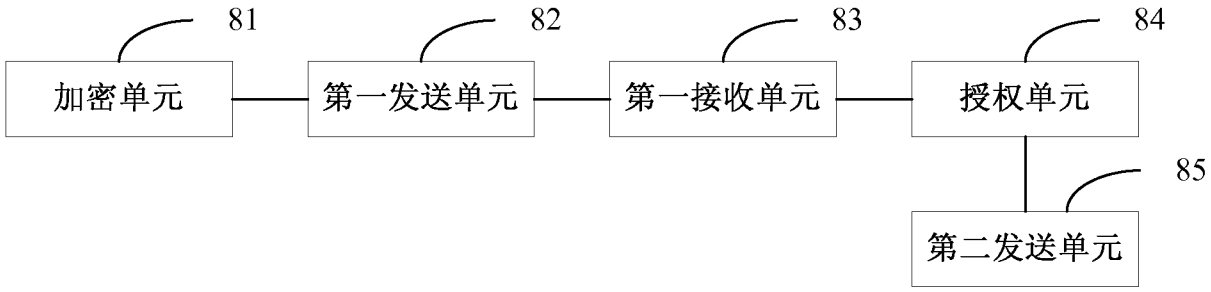
81
加密单元
82
第一发送单元
83
第一接收单元
84
授权单元
85
第二发送单元

图 8

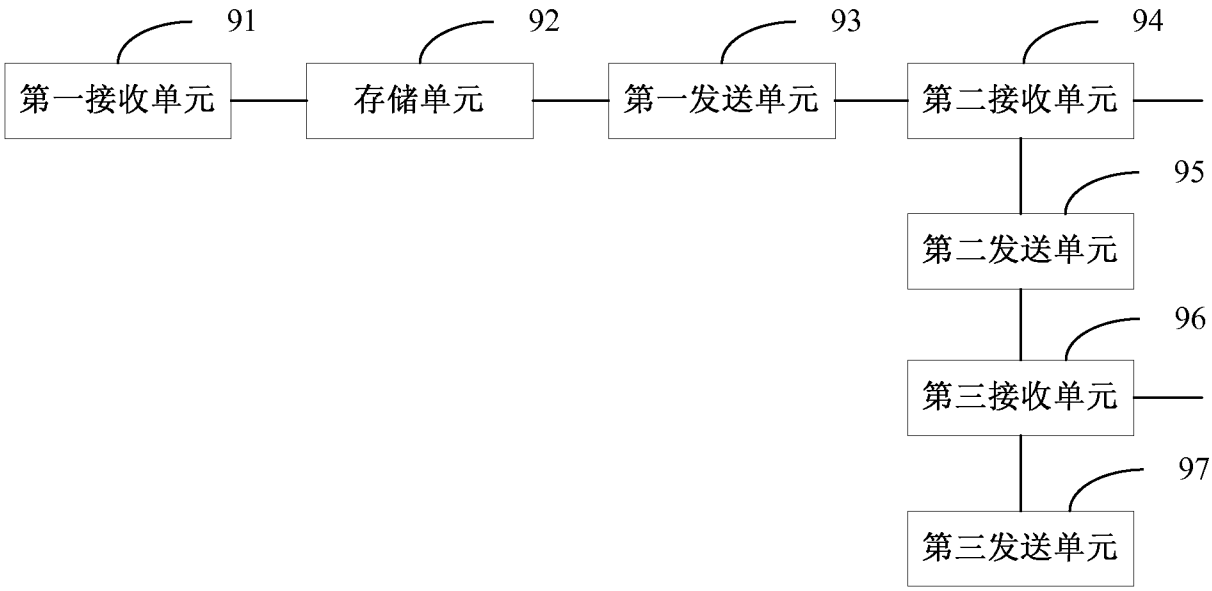
91
第一接收单元
92
存储单元
93
第一发送单元
94
第二接收单元
95
第二发送单元
96
第三接收单元
97
第三发送单元

图 9

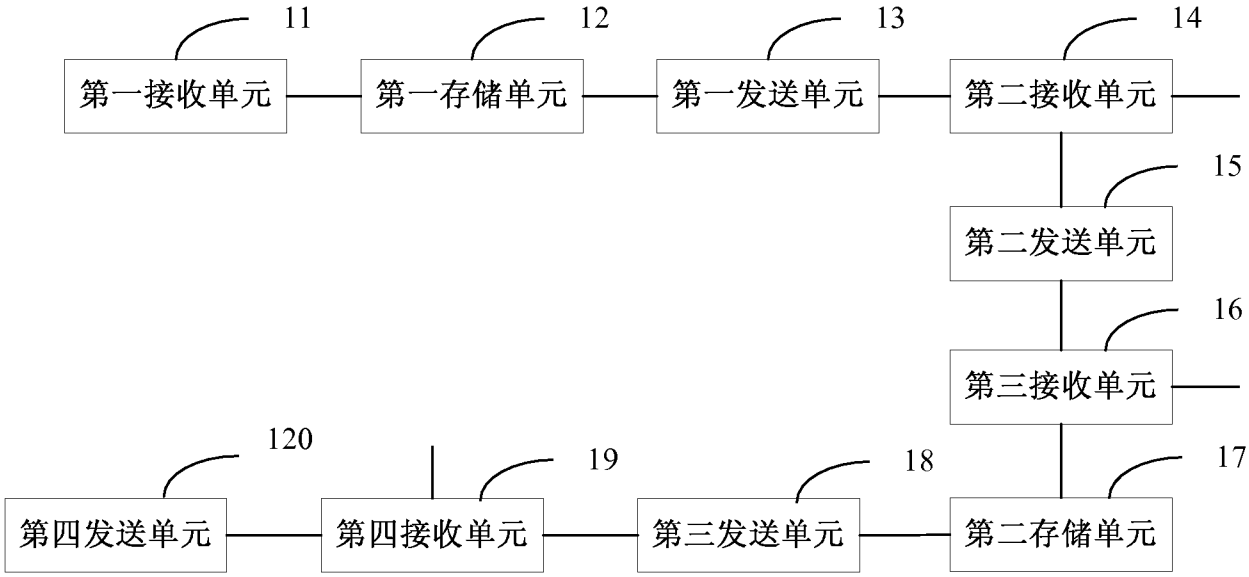
11
第一接收单元
12
第一存储单元
13
第一发送单元
14
第二接收单元
15
第二发送单元
16
第三接收单元
120
第四发送单元
19
第四接收单元
18
第三发送单元
17
第二存储单元

图 10

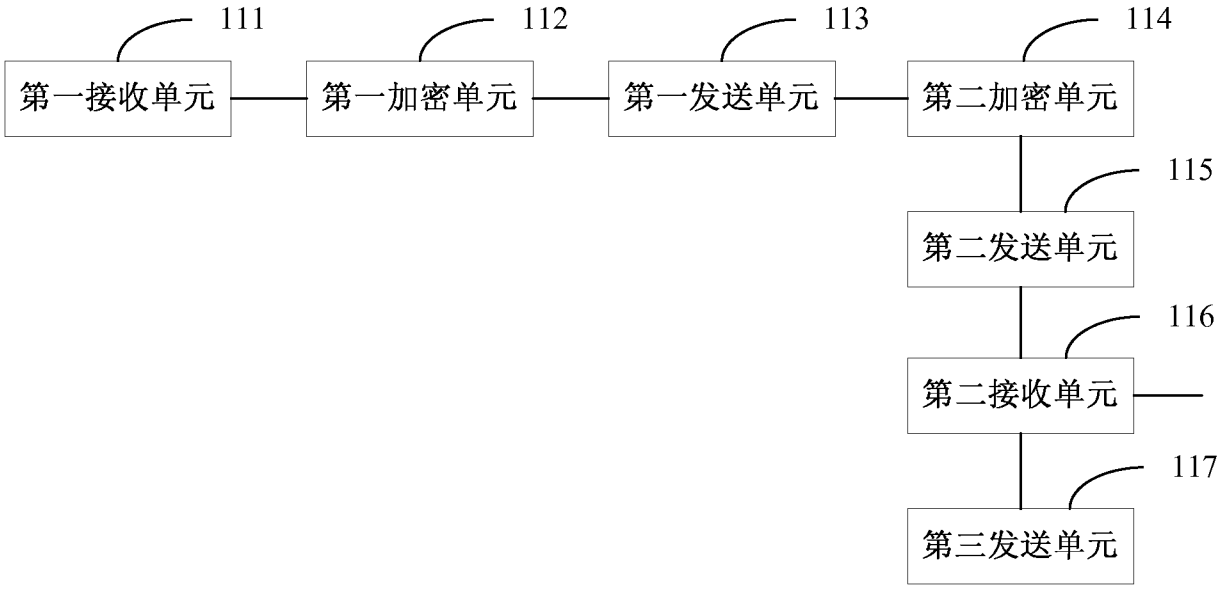
111
第一接收单元
112
第一加密单元
113
第一发送单元
114
第二加密单元
115
第二发送单元
116
第二接收单元
117
第三发送单元

图 11

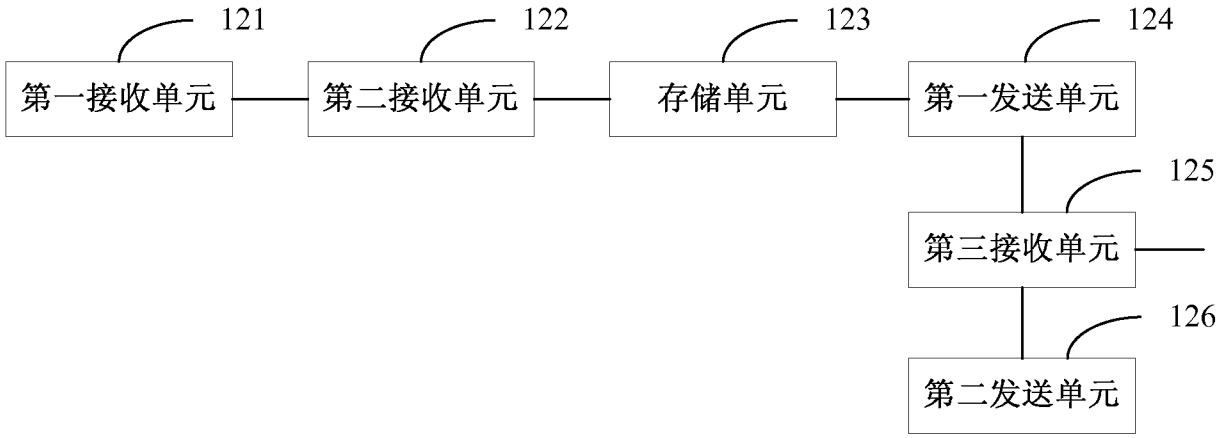
121
第一接收单元
122
第二接收单元
123
存储单元
124
第一发送单元
125
第三接收单元
126
第二发送单元

图 12

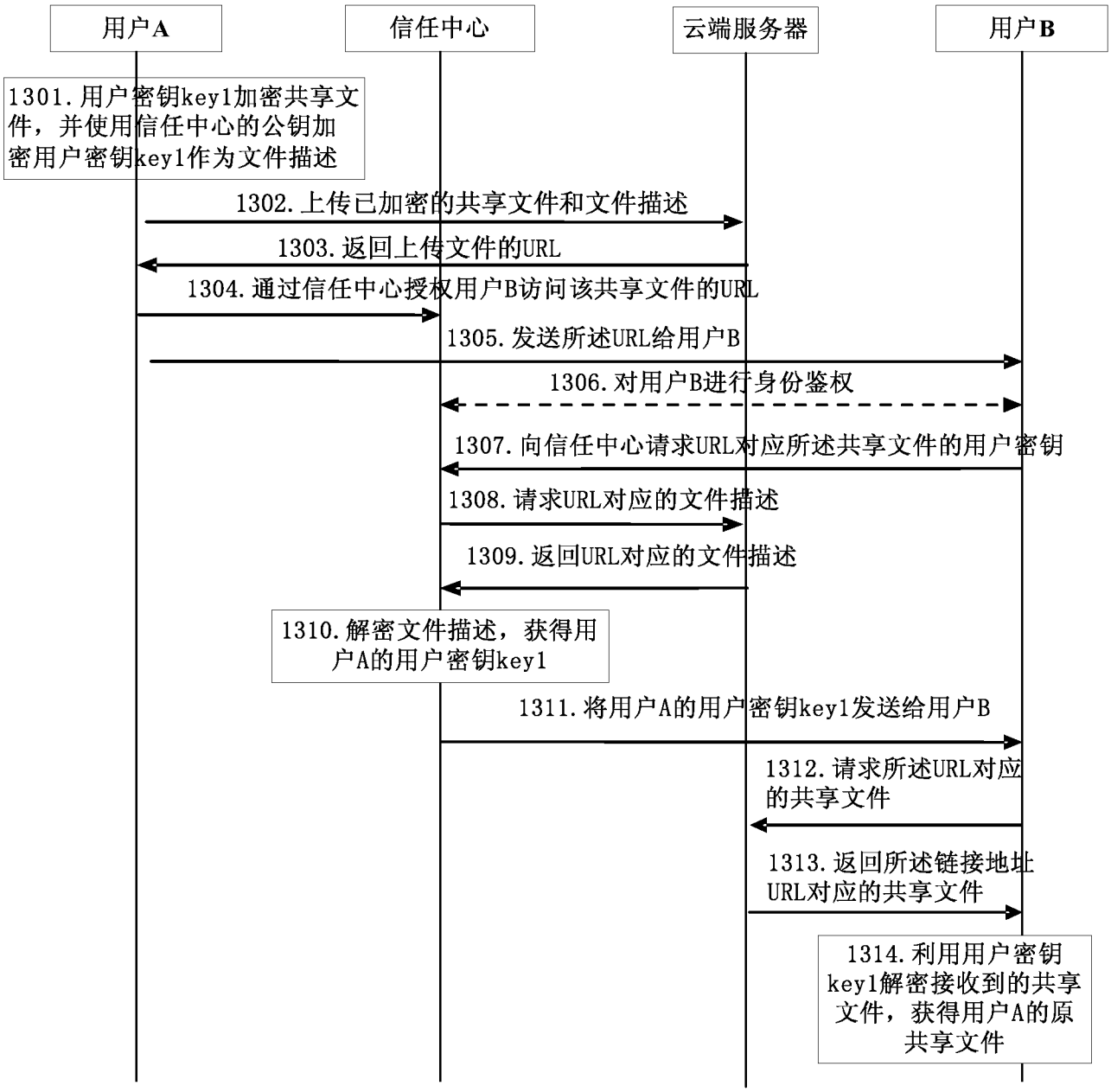
用户A
信任中心
云端服务器
用户B
1301.用户密钥key1加密共享文件，并使用信任中心的公钥加密用户密钥key1作为文件描述
1302.上传已加密的共享文件和文件描述
1303.返回上传文件的URL
1304.通过信任中心授权用户B访问该共享文件的URL
1305.发送所述URL给用户B
1306.对用户B进行身份鉴权
1307.向信任中心请求URL对应所述共享文件的用户密钥
1308.请求URL对应的文件描述
1309.返回URL对应的文件描述
1310.解密文件描述，获得用户A的用户密钥key1
1311.将用户A的用户密钥key1发送给用户B
1312.请求所述URL对应的共享文件
1313.返回所述链接地址URL对应的共享文件
1314.利用用户密钥key1解密接收到的共享文件，获得用户A的原共享文件

图 13

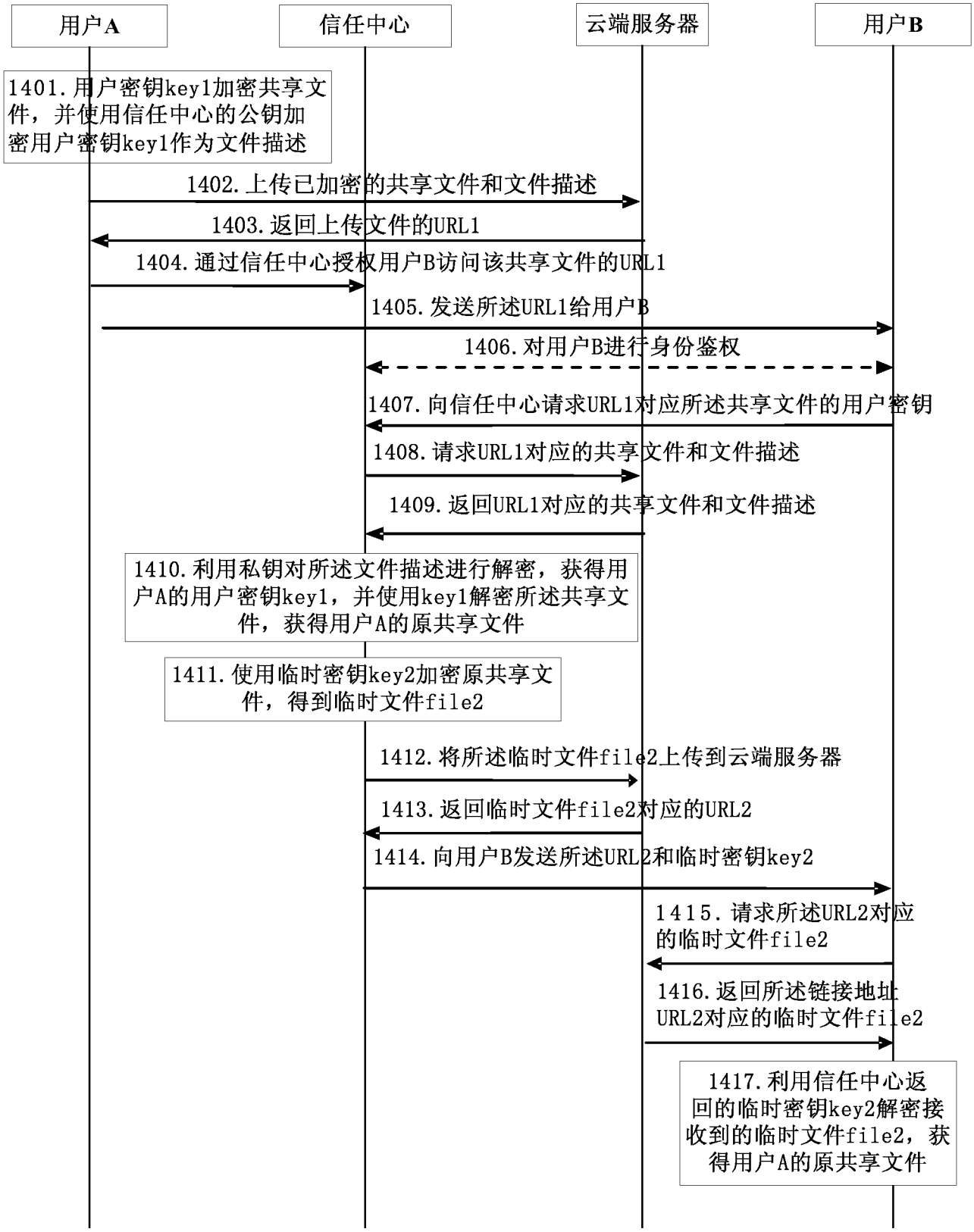
用户A
信任中心
云端服务器
用户B
1401.用户密钥key1加密共享文件，并使用信任中心的公钥加密用户密钥key1作为文件描述
1402.上传已加密的共享文件和文件描述
1403.返回上传文件的URL1
1404.通过信任中心授权用户B访问该共享文件的URL1
1405.发送所述URL1给用户B
1406.对用户B进行身份鉴权
1407.向信任中心请求URL1对应所述共享文件的用户密钥
1408.请求URL1对应的共享文件和文件描述
1409.返回URL1对应的共享文件和文件描述
1410.利用私钥对所述文件描述进行解密，获得用户A的用户密钥key1，并使用key1解密所述共享文件，获得用户A的原共享文件
1411.使用临时密钥key2加密原共享文件，得到临时文件file2
1412.将所述临时文件file2上传到云端服务器
1413.返回临时文件file2对应的URL2
1414.向用户B发送所述URL2和临时密钥key2
1415.请求所述URL2对应的临时文件file2
1416.返回所述链接地址URL2对应的临时文件file2
1417.利用信任中心返回的临时密钥key2解密接收到的临时文件file2，获得用户A的原共享文件

图 14

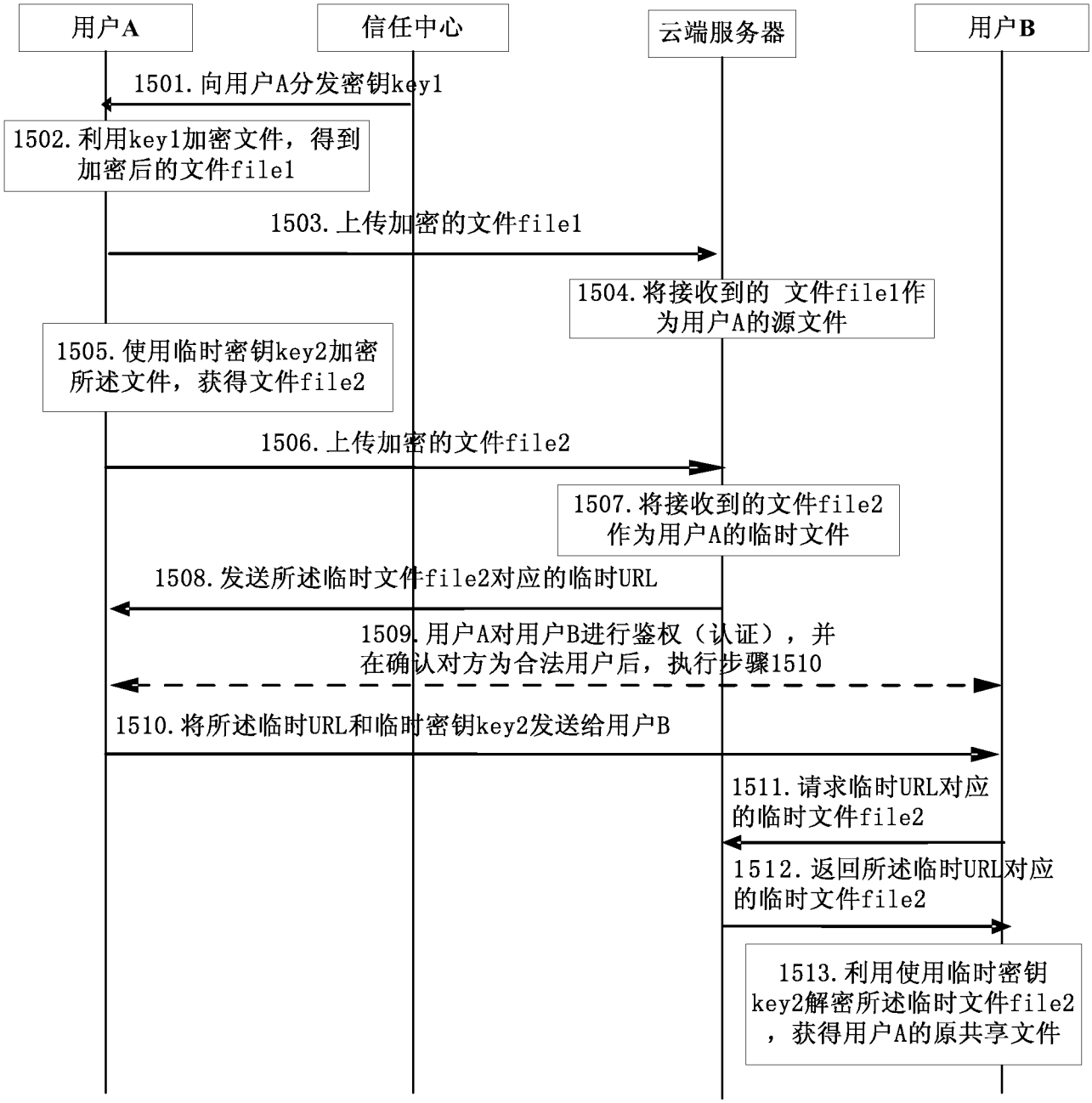
用户A
信任中心
云端服务器
用户B
1501.向用户A分发密钥key1
1502.利用key1加密文件，得到加密后的文件file1
1503.上传加密的文件file1
1504.将接收到的 文件file1作为用户A的源文件
1505.使用临时密钥key2加密所述文件，获得文件file2
1506.上传加密的文件file2
1507.将接收到的文件file2作为用户A的临时文件
1508.发送所述临时文件file2对应的临时URL
1509.用户A对用户B进行鉴权（认证），并在确认对方为合法用户后，执行步骤1510
1510.将所述临时URL和临时密钥key2发送给用户B
1511.请求临时URL对应的临时文件file2
1512.返回所述临时URL对应的临时文件file2
1513.利用使用临时密钥key2解密所述临时文件file2，获得用户A的原共享文件

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/070724

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (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)

IPC: H04

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)

VEN, CNKI, CPRSABS: cryptographic key, sharing, public key, private key, trust

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101833615 A (SHANGHAI YINGZHE INFORMATION SCIENCE & TECHNOLOGY CO., LTD.), 15 September 2010 (15.09.2010), description, pages 4-5	1-12

☐ 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	Date of mailing of the international search report
24 February 2014 (24.02.2014)	**13 March 2014 (13.03.2014)**
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 **ZHU, Shaohua** Telephone No.: (86-10) **62411229**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/070724

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101833615 A	15.09.2010	None	

国际检索报告

国际申请号
PCT/CN2014/070724

A. 主题的分类

H04L9/00(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)

IPC:H04

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）)

VEN,CNKI,CPRSABS:共享，密钥，信任，公钥，私钥，sharing，public key，private key，trust

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	CN101833615A(上海盈哲信息科技有限公司) 15.9 月 2010（15.09.2010） 说明书第 4-5 页	1-12

☐ 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	国际检索报告邮寄日期
24.2 月 2014（24.02.2014）	**13.3 月 2014 (13.03.2014)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 朱少华 电话号码：(86-10) **62411229**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2014/070724

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101833615A	15.09.2010	无	