(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115333813 A
(43)申请公布日 2022.11.11

(21)申请号 202210921196.2

(22)申请日 2022.08.02

(71)申请人 中国电信股份有限公司
地址 100033 北京市西城区金融大街31号

(72)发明人 玄勇 蒋艳军 赵轶新 孙科

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
专利代理师 莎日娜

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)

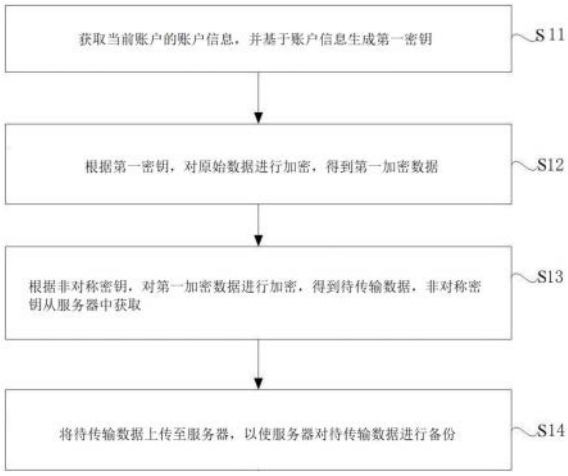
权利要求书2页 说明书9页 附图3页

(54)发明名称

一种数据加密传输方法、装置、电子设备及存储介质

(57)摘要

本公开关于一种数据加密传输方法、装置、电子设备及存储介质，包括：获取当前账户的账户信息，并基于账户信息生成第一密钥；根据第一密钥，对原始数据进行加密，得到第一加密数据；根据非对称密钥，对第一加密数据进行加密，得到待传输数据，非对称密钥从服务器中获取；将待传输数据上传至服务器，以使服务器对待传输数据进行备份。这样，采用第一密钥和非对称密钥，对原始数据进行加密方式不同的多层加密，可以大大降低数据泄漏的风险，而且，第一密钥是在客户端本地生成的，并不会被上传至服务器中，这样，在服务器端就无法对待传输数据进行解密，从而进一步提高了数据安全性。



CN 115333813 A

1.一种数据加密传输方法,其特征在于,应用于客户端,包括:

获取当前账户的账户信息,并基于所述账户信息生成第一密钥;

根据所述第一密钥,对原始数据进行加密,得到第一加密数据;

根据非对称密钥,对所述第一加密数据进行加密,得到待传输数据,所述非对称密钥从服务器中获取;

将所述待传输数据上传至所述服务器,以使所述服务器对所述待传输数据进行备份。

2.根据权利要求1所述的数据加密传输方法,其特征在于,在所述根据所述第一密钥,对原始数据进行加密,得到第一加密数据之后,所述方法还包括:

根据预设加密算法,生成第二密钥;

根据所述第二密钥,对所述第一加密数据进行加密,得到第二加密数据;

所述根据非对称密钥,对所述第一加密数据进行加密,得到待传输数据,包括:

根据非对称密钥,对所述第二加密数据进行加密,得到待传输数据。

3.根据权利要求2所述的数据加密传输方法,其特征在于,所述根据所述第一密钥,对原始数据进行加密,得到第一加密数据,包括:

根据所述第一密钥,对每条原始数据单独进行加密,得到每条原始数据分别对应的第一加密数据;

所述根据所述第二密钥,对所述第一加密数据进行加密,得到第二加密数据,包括:

将所述第一加密数据组成集合;

根据所述第二密钥,对所述集合进行加密,得到第二加密数据。

4.根据权利要求1所述的数据加密传输方法,其特征在于,所述根据非对称密钥,对所述第一加密数据进行加密,得到待传输数据,包括:

获取所述当前账户的候选信息;

根据非对称密钥,对所述第一加密数据及所述候选信息进行加密,得到待传输数据。

5.根据权利要求1所述的数据加密传输方法,其特征在于,在所述将所述待传输数据上传至所述服务器之后,所述方法还包括:

响应于预设下载操作,从所述服务器下载所述待传输数据;

根据所述非对称密钥,对所述待传输数据进行解密,得到所述第一加密数据;

根据所述第一密钥,对所述第一加密数据进行解密,得到所述原始数据。

6.一种数据加密传输装置,其特征在于,应用于客户端,包括:

获取单元,被配置为执行获取当前账户的账户信息,并基于所述账户信息生成第一密钥;

第一加密单元,被配置为执行根据所述第一密钥,对原始数据进行加密,得到第一加密数据;

非对称加密单元,被配置为执行根据非对称密钥,对所述第一加密数据进行加密,得到待传输数据,所述非对称密钥从服务器中获取;

传输单元,被配置为执行将所述待传输数据上传至所述服务器,以使所述服务器对所述待传输数据进行备份。

7.根据权利要求6所述的数据加密传输装置,其特征在于,所述装置还包括:

第二加密单元,被配置为执行根据预设加密算法,生成第二密钥;根据所述第二密钥,

对所述第一加密数据进行加密，得到第二加密数据；

所述非对称加密单元，具体被配置为执行根据非对称密钥，对所述第二加密数据进行加密，得到待传输数据。

8.根据权利要求7所述的数据加密传输装置，其特征在于，

所述第一加密单元，具体被配置为执行根据所述第一密钥，对每条原始数据单独进行加密，得到每条原始数据分别对应的第一加密数据；

所述第二加密单元，具体被配置为执行将所述第一加密数据组成集合；根据所述第二密钥，对所述集合进行加密，得到第二加密数据。

9.根据权利要求6所述的数据加密传输装置，其特征在于，所述非对称加密单元，具体被配置为执行：

获取所述当前账户的候选信息；

根据非对称密钥，对所述第一加密数据及所述候选信息进行加密，得到待传输数据。

10.根据权利要求6所述的数据加密传输装置，其特征在于，所述装置还包括：

解密单元，被配置为执行响应于预设下载操作，从所述服务器下载所述待传输数据；根据所述非对称密钥，对所述待传输数据进行解密，得到所述第一加密数据；根据所述第一密钥，对所述第一加密数据进行解密，得到所述原始数据。

11.一种电子设备，其特征在于，包括：

处理器；

用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为执行所述指令，以实现如权利要求1至5中任一项所述的数据加密传输方法。

12.一种计算机可读存储介质，其特征在于，当所述计算机可读存储介质中的指令由数据加密传输电子设备的处理器执行时，使得数据加密传输电子设备能够执行如权利要求1至5中任一项所述的数据加密传输方法。

一种数据加密传输方法、装置、电子设备及存储介质

技术领域

[0001] 本公开涉及数据传输领域，尤其涉及一种数据加密传输方法、装置、电子设备及存储介质。

背景技术

[0002] 在许多场景中，用户经常需要利用网络进行通信，从客户端向服务器上传数据或从服务器下载数据，因此，数据安全变得越来越重要，一旦上传的数据被窃取，后果将不堪设想。通常，可以通过对数据进行加密传输，来维护数据的安全性。

[0003] 现有技术中，通常在客户端向服务器传输数据前，由服务器向客户端提供密钥，然后，客户端根据获取到的密钥，对数据进行加密，再将加密后的数据上传至服务器，当需要获取数据时，可以再利用密钥对加密后的数据进行解密。

[0004] 但是，在上述数据加密传输方法中，客户端和服务器中都存储着密钥，如果一方存在密钥泄露问题，就会导致传输的数据不安全，因此，数据泄露的风险较高，数据安全难以得到保障。

发明内容

[0005] 本公开提供一种待处理数据加密传输方法、装置、电子设备及存储介质，以至少解决相关技术中数据泄露的风险较高，数据安全难以得到保障的问题。本公开的技术方案如下：

[0006] 根据本公开实施例的第一方面，提供一种数据加密传输方法，应用于客户端，包括：

[0007] 获取当前账户的账户信息，并基于所述账户信息生成第一密钥；

[0008] 根据所述第一密钥，对原始数据进行加密，得到第一加密数据；

[0009] 根据非对称密钥，对所述第一加密数据进行加密，得到待传输数据，所述非对称密钥从服务器中获取；

[0010] 将所述待传输数据上传至所述服务器，以使所述服务器对所述待传输数据进行备份。

[0011] 可选的，在所述根据所述第一密钥，对原始数据进行加密，得到第一加密数据之后，所述方法还包括：

[0012] 根据预设加密算法，生成第二密钥；

[0013] 根据所述第二密钥，对所述第一加密数据进行加密，得到第二加密数据；

[0014] 所述根据非对称密钥，对所述第一加密数据进行加密，得到待传输数据，包括：

[0015] 根据非对称密钥，对所述第二加密数据进行加密，得到待传输数据。

[0016] 可选的，所述根据所述第一密钥，对原始数据进行加密，得到第一加密数据，包括：

[0017] 根据所述第一密钥，对每条原始数据单独进行加密，得到每条原始数据分别对应的第一加密数据；

[0018] 所述根据所述第二密钥，对所述第一加密数据进行加密，得到第二加密数据，包括：

[0019] 将所述第一加密数据组成集合；

[0020] 根据所述第二密钥，对所述集合进行加密，得到第二加密数据。

[0021] 可选的，所述根据非对称密钥，对所述第一加密数据进行加密，得到待传输数据，包括：

[0022] 获取所述当前账户的候选信息；

[0023] 根据非对称密钥，对所述第一加密数据及所述候选信息进行加密，得到待传输数据。

[0024] 可选的，在所述将所述待传输数据上传至所述服务器之后，所述方法还包括：

[0025] 响应于预设下载操作，从所述服务器下载所述待传输数据；

[0026] 根据所述非对称密钥，对所述待传输数据进行解密，得到所述第一加密数据；

[0027] 根据所述第一密钥，对所述第一加密数据进行解密，得到所述原始数据。

[0028] 根据本公开实施例的第二方面，提供一种数据加密传输装置，应用于客户端，包括：

[0029] 获取单元，被配置为执行获取当前账户的账户信息，并基于所述账户信息生成第一密钥；

[0030] 第一加密单元，被配置为执行根据所述第一密钥，对原始数据进行加密，得到第一加密数据；

[0031] 非对称加密单元，被配置为执行根据非对称密钥，对所述第一加密数据进行加密，得到待传输数据，所述非对称密钥从服务器中获取；

[0032] 传输单元，被配置为执行将所述待传输数据上传至所述服务器，以使所述服务器对所述待传输数据进行备份。

[0033] 可选的，所述装置还包括：

[0034] 第二加密单元，被配置为执行根据预设加密算法，生成第二密钥；根据所述第二密钥，对所述第一加密数据进行加密，得到第二加密数据；

[0035] 所述非对称加密单元，具体被配置为执行根据非对称密钥，对所述第二加密数据进行加密，得到待传输数据。

[0036] 可选的，所述第一加密单元，具体被配置为执行根据所述第一密钥，对每条原始数据单独进行加密，得到每条原始数据分别对应的第一加密数据；

[0037] 所述第二加密单元，具体被配置为执行将所述第一加密数据组成集合；根据所述第二密钥，对所述集合进行加密，得到第二加密数据。

[0038] 可选的，所述非对称加密单元，具体被配置为执行：

[0039] 获取所述当前账户的候选信息；

[0040] 根据非对称密钥，对所述第一加密数据及所述候选信息进行加密，得到待传输数据。

[0041] 可选的，所述装置还包括：

[0042] 解密单元，被配置为执行响应于预设下载操作，从所述服务器下载所述待传输数据；根据所述非对称密钥，对所述待传输数据进行解密，得到所述第一加密数据；根据所述

第一密钥，对所述第一加密数据进行解密，得到所述原始数据。

[0043] 根据本公开实施例的第三方面，提供一种数据加密传输电子设备，包括：

[0044] 处理器；

[0045] 用于存储所述处理器可执行指令的存储器；

[0046] 其中，所述处理器被配置为执行所述指令，以实现上述任一项所述的数据加密传输方法。

[0047] 根据本公开实施例的第四方面，提供一种计算机可读存储介质，当所述计算机可读存储介质中的指令由数据加密传输电子设备的处理器执行时，使得数据加密传输电子设备能够执行上述任一所述的数据加密传输方法。

[0048] 根据本公开实施例的第五方面，提供一种计算机程序产品，包括计算机程序/指令，所述计算机程序/指令被处理器执行时实现上述任一项所述的数据加密传输方法。

[0049] 本公开的实施例提供的技术方案至少带来以下有益效果：

[0050] 获取当前账户的账户信息，并基于账户信息生成第一密钥；根据第一密钥，对原始数据进行加密，得到第一加密数据；根据非对称密钥，对第一加密数据进行加密，得到待传输数据，非对称密钥从服务器中获取；将待传输数据上传至服务器，以使服务器对待传输数据进行备份。

[0051] 这样，采用第一密钥和非对称密钥，对原始数据进行加密方式不同的多层加密，可以大大降低数据泄漏的风险，而且，第一密钥是在客户端本地生成的，并不会被上传至服务器中，这样，在服务器端就无法对待传输数据进行解密，从而进一步提高了数据安全性。

[0052] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

[0053] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理，并不构成对本公开的不当限定。

[0054] 图1是根据一示例性实施例示出的一种数据加密传输方法的流程图。

[0055] 图2是根据一示例性实施例示出的一种数据加密传输方法的方案示意图。

[0056] 图3是根据一示例性实施例示出的一种数据加密传输装置的框图。

[0057] 图4是根据一示例性实施例示出的一种用于数据加密传输的电子设备的框图。

[0058] 图5是根据一示例性实施例示出的一种用于数据加密传输的装置的框图。

具体实施方式

[0059] 为了使本领域普通人员更好地理解本公开的技术方案，下面将结合附图，对本公开实施例中的技术方案进行清楚、完整地描述。

[0060] 需要说明的是，本公开的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本公开的实施例能够以除了在这里图示或描述的那些以外的顺序实施。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面

相一致的装置和方法的例子。

[0061] 图1是根据一示例性实施例示出的一种数据加密传输方法的流程图，如图1所示，该数据加密传输方法应用于客户端，包括以下步骤。

[0062] 在步骤S11中，获取当前账户的账户信息，并基于账户信息生成第一密钥。

[0063] 在许多场景中，用户经常需要利用网络进行通信，从客户端向服务器上传数据或从服务器下载数据，为了在数据传输过程中维护数据安全，减少数据被泄露的风险，通常，可以通过对数据进行加密传输。

[0064] 在本步骤中，可以根据当前账户的账户信息，生成第一密钥，第一密钥用于对原始数据进行加密。其中，当前账户的账户信息可以包括但不限于当前账户对应的账户名、密码、所属地区、性别、年龄等信息，具体不做限定。

[0065] 其中，基于账户信息生成第一密钥的步骤中，可以先采用MD5(MD5 Message-Digest Algorith，MD5消息摘要算法)，对当前账户的多项账户信息分别进行处理，得到多个初始字符串，然后，对多个初始字符串进行拼接，得到第一密钥。

[0066] 在本公开中，第一密钥可以存储在客户端本地，比如，可以存储至客户端本地的local.properties文件中，或者，也可以存储至第三方设备或第三方数据库中进行备份。

[0067] 在步骤S12中，根据第一密钥，对原始数据进行加密，得到第一加密数据。

[0068] 在生成第一密钥之后，可以根据第一密钥，对原始数据进行加密，得到第一加密数据。可以理解，第一密钥是在客户端本地生成的，后续并不会上传至服务器，因此，利用第一密钥对原始数据进行加密之后，服务器端即使获取到第一加密数据，也无法对第一加密数据进行解密，还原出原始数据，从而可以提高数据的安全性，减少数据泄露的可能性。

[0069] 其中，根据第一密钥对原始数据进行加密，可以采取任意一种预设的对称加密算法，对称加密算法是指加密和解密采用相同密钥的算法，如AES(Advanced Encryption Standard，高阶加密标准)算法、DES(Data Encryption Standard，数据加密标准)算法或TEDS(Triple Data Encryption Algorithm，三重数据加密算法)等等，具体不做限定。

[0070] 一种实现方式中，在根据第一密钥，对原始数据进行加密，得到第一加密数据之后，方法还包括：根据预设加密算法，生成第二密钥；根据第二密钥，对第一加密数据进行加密，得到第二加密数据。

[0071] 也就是说，在根据第一密钥，对原始数据进行一层加密的基础上，进一步进行二层加密，根据客户端本地生成的第二密钥，对第一加密数据进行进一步加密，得到第二加密数据。其中，第二密钥可以是随机生成的，也可以是基于对第一加密数据生成的，具体不做限定。可以理解，第二密钥后续也不会上传至服务器，因此，利用第二密钥对第一加密数据进行进一步加密之后，服务器端通过数据解密还原出原始数据的概率更低，因此可以进一步提高数据的安全性，减少数据泄露的可能性。

[0072] 其中，根据第一密钥，对原始数据进行加密，得到第一加密数据，包括：根据第一密钥，对每条原始数据单独进行加密，得到每条原始数据分别对应的第一加密数据；根据第二密钥，对第一加密数据进行加密，得到第二加密数据，包括：将第一加密数据组成集合；根据第二密钥，对集合进行加密，得到第二加密数据。

[0073] 也就是说，在包括多条原始数据的情况下，第一密钥和第二密钥的加密方式有所不同，首先，由第一密钥对每条原始数据单独进行加密，然后，由第二密钥对多条第一加密

数据组成的集合进行加密，得到第二加密数据。这样，对原始数据的加密方式更为多样，有利于进一步提高数据的安全性。

[0074] 在步骤S13中，根据非对称密钥，对第一加密数据进行加密，得到待传输数据，非对称密钥从服务器中获取。

[0075] 在本公开中，客户端还可以从服务器中获取非对称密钥，在得到第一加密数据之后，利用非对称密钥对第一加密数据进行加密，得到待传输数据。其中，非对称密钥即为非对称加密算法中所需要的密钥，在非对称加密算法中，需要两个密钥分别进行加密和解密，这两个密钥是公开密钥(public key，公钥)和私有密钥(private key，私钥)，公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。

[0076] 其中，非对称密钥可以是预设的与当前账户对应的，或者，也可以先由客户端向服务器发送数据传输请求，服务器响应于客户端发送的数据传输请求，随机生成并返回至客户端的，具体不做限定。

[0077] 一种实现方式中，若在本步骤之前，已经对原始数据进行了两层加密，那么，在本步骤中，客户端可以根据非对称密钥，对第二加密数据进行加密，得到待传输数据。这样，就实现了对原始数据的三层加密，进一步提高了数据的安全性。

[0078] 一种实现方式中，根据非对称密钥，对第一加密数据进行加密，得到待传输数据，包括：获取当前账户的候选信息；根据非对称密钥，对第一加密数据及候选信息进行加密，得到待传输数据。

[0079] 也就是说，在本步骤中，非对称密钥除了用于对第一加密数据进行加密，还可以对当前账户的候选信息进行加密，候选信息可以是当前账户对应的除账户信息之外的其他任意信息，包括但不限于操作数据、偏好信息，等等，可以根据需求进行设定，具体不做限定。候选信息相比于原始信息，通常具有较低的数据安全等级，因此，仅利用非对称密钥进行加密，可以在维持数据安全的前提下减少系统的计算量，提高数据传输效率。

[0080] 在步骤S14中，将待传输数据上传至服务器，以使服务器对待传输数据进行备份。

[0081] 由前述可知，对原始数据进行多层加密之后，得到待传输数据，那么，在本步骤中，可以将待传输数据上传至服务器，进而，服务器可以对待传输数据进行备份，客户端可以在需要时从服务器获取待传输数据，并对数据进行还原，得到原始数据。可以理解，在服务器端，并未获取到第一密钥及第二密钥，因此，服务器端无法对原始数据进行还原，即使服务器端发生数据泄露，原始数据也不会泄露，从而可以提高数据安全性。

[0082] 一种实现方式中，在将待传输数据上传至服务器之后，还可以：响应于预设下载操作，从服务器下载待传输数据；根据非对称密钥，对待传输数据进行解密，得到第一加密数据；根据第一密钥，对第一加密数据进行解密，得到原始数据。

[0083] 也就是说，当用户需要下载原始数据时，可以在客户端执行预设下载操作，然后，客户端响应于预设下载操作，从服务器下载待传输数据；根据非对称密钥，对待传输数据进行解密，得到第一加密数据；根据第一密钥，对第一加密数据进行解密，得到原始数据。其中，在对原始数据进行三层加密的情况下，在根据非对称密钥，对待传输数据进行解密后，得到第二加密数据，再利用第二密钥对第二加密数据进行解密，才能得到第一加密数据。可以理解，解密所用的算法与前述步骤中的加密算法一一对应，本公开对此不做限定。

[0084] 举例而言，如图2所示，为本公开提供的一种方案示意图，该方案为一种基于客户端联系人上传三层加密的方法，对用户联系人实现层层加密，保证用户联系人上传到服务器的联系人是不被解密和破解的，具体技术方案如下：

[0085] 首先，客户端在本地可以根据用户个人信息拼接生成MD5字符串，把生成的MD5字符串存储到客户端local.properties文件中，该字符串为密钥1，使用密钥1对用户每一条联系人信息都进行加密；然后，把用户所有单独加密过的联系人放入到集合当中，使用特定的公式生成一串密钥，该密钥为密钥2，存储在客户端local.properties文件中，使用密钥2对集合进行整体加密；进而，将加密的集合和用户其他信息使用非对称密钥加密上传至服务器，该非对称密钥由服务器提供。

[0086] 可以理解，将此方法应用于客户端联系人上传中，对用户联系人进行层层加密，使得用户联系人数据在服务器中不被破解。而且采用三层加密，第一层和第二层生成不同的密钥，并将密钥存储在客户端local.properties文件中，使第一密钥和第二密钥被窃取和泄漏的概率降低，大大提升了数据安全性。

[0087] 由以上可见，本公开的实施例提供的技术方案，采用第一密钥和非对称密钥，对原始数据进行加密方式不同的多层加密，可以大大降低数据泄漏的风险，而且，第一密钥是在客户端本地生成的，并不会被上传至服务器中，这样，在服务器端就无法对待传输数据进行解密，从而进一步提高了数据安全性。

[0088] 图3是根据一示例性实施例示出的一种数据加密传输装置框图，应用于客户端，该装置包括：

[0089] 获取单元201，被配置为执行获取当前账户的账户信息，并基于所述账户信息生成第一密钥；

[0090] 第一加密单元202，被配置为执行根据所述第一密钥，对原始数据进行加密，得到第一加密数据；

[0091] 非对称加密单元203，被配置为执行根据非对称密钥，对所述第一加密数据进行加密，得到待传输数据，所述非对称密钥从服务器中获取；

[0092] 传输单元204，被配置为执行将所述待传输数据上传至所述服务器，以使所述服务器对所述待传输数据进行备份。

[0093] 一种实现方式中，所述装置还包括：

[0094] 第二加密单元，被配置为执行根据预设加密算法，生成第二密钥；根据所述第二密钥，对所述第一加密数据进行加密，得到第二加密数据；

[0095] 所述非对称加密单元203，具体被配置为执行根据非对称密钥，对所述第二加密数据进行加密，得到待传输数据。

[0096] 一种实现方式中，所述第一加密单元202，具体被配置为执行根据所述第一密钥，对每条原始数据单独进行加密，得到每条原始数据分别对应的第一加密数据；

[0097] 所述第二加密单元，具体被配置为执行将所述第一加密数据组成集合；根据所述第二密钥，对所述集合进行加密，得到第二加密数据。

[0098] 一种实现方式中，所述非对称加密单元203，具体被配置为执行：

[0099] 获取所述当前账户的候选信息；

[0100] 根据非对称密钥，对所述第一加密数据及所述候选信息进行加密，得到待传输数

据。

[0101] 一种实现方式中,所述装置还包括:

[0102] 解密单元,被配置为执行响应于预设下载操作,从所述服务器下载所述待传输数据;根据所述非对称密钥,对所述待传输数据进行解密,得到所述第一加密数据;根据所述第一密钥,对所述第一加密数据进行解密,得到所述原始数据。

[0103] 由以上可见,本公开的实施例提供的技术方案,采用第一密钥和非对称密钥,对原始数据进行加密方式不同的多层加密,可以大大降低数据泄漏的风险,而且,第一密钥是在客户端本地生成的,并不会被上传至服务器中,这样,在服务器端就无法对待传输数据进行解密,从而进一步提高了数据安全性。

[0104] 关于上述实施例中的装置,其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述,此处将不做详细阐述说明。

[0105] 图4是根据一示例性实施例示出的一种用于数据加密传输的电子设备的框图,包括处理器和存储器,其中,存储器用于存放计算机程序;处理器用于执行存储器上所存放的程序。

[0106] 存储器可以包括随机存取存储器(Random Access Memory,简称RAM),也可以包括非易失性存储器(non-volatile memory),例如至少一个磁盘存储器。可选的,存储器还可以是至少一个位于远离前述处理器的存储装置。

[0107] 上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit,简称CPU)、网络处理器(Network Processor,简称NP)等;还可以是数字信号处理器(Digital Signal Processing,简称DSP)、专用集成电路(Application Specific Integrated Circuit,简称ASIC)、现场可编程门阵列(Field-Programmable Gate Array,简称FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0108] 在示例性实施例中,还提供了一种包括指令的计算机可读存储介质,例如包括指令的存储器,上述指令可由电子设备的处理器执行以完成上述方法。可选地,计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0109] 在示例性实施例中,还提供一种计算机程序产品,当其在计算机上运行时,使得计算机实现上述待处理数据加密传输的方法。

[0110] 由以上可见,本公开的实施例提供的技术方案,采用第一密钥和非对称密钥,对原始数据进行加密方式不同的多层加密,可以大大降低数据泄漏的风险,而且,第一密钥是在客户端本地生成的,并不会被上传至服务器中,这样,在服务器端就无法对待传输数据进行解密,从而进一步提高了数据安全性。

[0111] 图5是根据一示例性实施例示出的一种用于数据加密传输的装置800的框图。

[0112] 例如,装置800可以是移动电话,计算机,数字广播电子设备,消息收发设备,游戏控制台,平板设备,医疗设备,健身设备,个人数字助理等。

[0113] 参照图5,装置800可以包括以下一个或多个组件:处理组件802,存储器804,电力组件806,多媒体组件808,音频组件810,输入/输出(I/O)的接口812,传感器组件814,以及通信组件816。

[0114] 处理组件802通常控制装置800的整体操作,诸如与显示,电话呼叫,数据通信,相机操作和记录操作相关联的操作。处理组件802可以包括一个或多个处理器820来执行指

令，以完成上述的方法的全部或部分步骤。此外，处理组件802可以包括一个或多个模块，便于处理组件802和其他组件之间的交互。例如，处理组件802可以包括多媒体模块，以方便多媒体组件808和处理组件802之间的交互。

[0115] 存储器804被配置为存储各种类型的数据以支持在设备800的操作。这些数据的示例包括用于在装置800上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器804可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(SRAM)，电可擦除可编程只读存储器(EEPROM)，可擦除可编程只读存储器(EPROM)，可编程只读存储器(PROM)，只读存储器(ROM)，磁存储器，快闪存储器，磁盘或光盘。

[0116] 电源组件807为装置800的各种组件提供电力。电源组件807可以包括电源管理系统，一个或多个电源，及其他与为装置800生成、管理和分配电力相关联的组件。

[0117] 多媒体组件808包括在所述装置800和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器(LCD)和触摸面板(TP)。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件808包括一个前置摄像头和/或后置摄像头。当设备800处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的待处理多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0118] 音频组件810被配置为输出和/或输入音频信号。例如，音频组件810包括一个麦克风(MIC)，当装置800处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器804或经由通信组件816发送。在一些实施例中，音频组件810还包括一个扬声器，用于输出音频信号。

[0119] I/O接口812为处理组件802和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

[0120] 传感器组件814包括一个或多个传感器，用于为装置800提供各个方面的状态评估。例如，传感器组件814可以检测到设备800的打开/关闭状态，组件的相对定位，例如所述组件为装置800的显示器和小键盘，传感器组件814还可以检测装置800或装置800一个组件的位置改变，用户与装置800接触的存在或不存在，装置800方位或加速/减速和装置800的温度变化。传感器组件814可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件814还可以包括光传感器，如CMOS或CCD图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件814还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

[0121] 通信组件816被配置为便于装置800和其他设备之间有线或无线方式的通信。装置800可以接入基于通信标准的无线网络，如WiFi，运营商网络(如2G、3G、4G或5G)，或它们的组合。在一个示例性实施例中，通信组件816经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件816还包括近场通信(NFC)模块，以促进短程通信。例如，在NFC模块可基于射频识别(RFID)技术，红外数据协会(IrDA)

技术,超宽带(UWB)技术,蓝牙(BT)技术和其他技术来实现。

[0122] 在示例性实施例中,装置800可以被一个或多个应用专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子元件实现,用于执行第一方面和第二方面所述的方法。

[0123] 在示例性实施例中,还提供了一种包括指令的非临时性计算机可读存储介质,例如包括指令的存储器804,上述指令可由装置800的处理器820执行以完成上述方法。可选地,例如,存储介质可以是非临时性计算机可读存储介质,例如,所述非临时性非临时性计算机可读存储介质计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0124] 在示例性实施例中,还提供了一种包含指令的计算机程序产品,当其在计算机上运行时,使得计算机执行上述实施例中任一所述的数据加密传输方法。

[0125] 由以上可见,本公开的实施例提供的技术方案,采用第一密钥和非对称密钥,对原始数据进行加密方式不同的多层加密,可以大大降低数据泄漏的风险,而且,第一密钥是在客户端本地生成的,并不会被上传至服务器中,这样,在服务器端就无法对待传输数据进行解密,从而进一步提高了数据安全性。

[0126] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本公开的真正范围和精神由下面的权利要求指出。

[0127] 应当理解的是,本公开并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

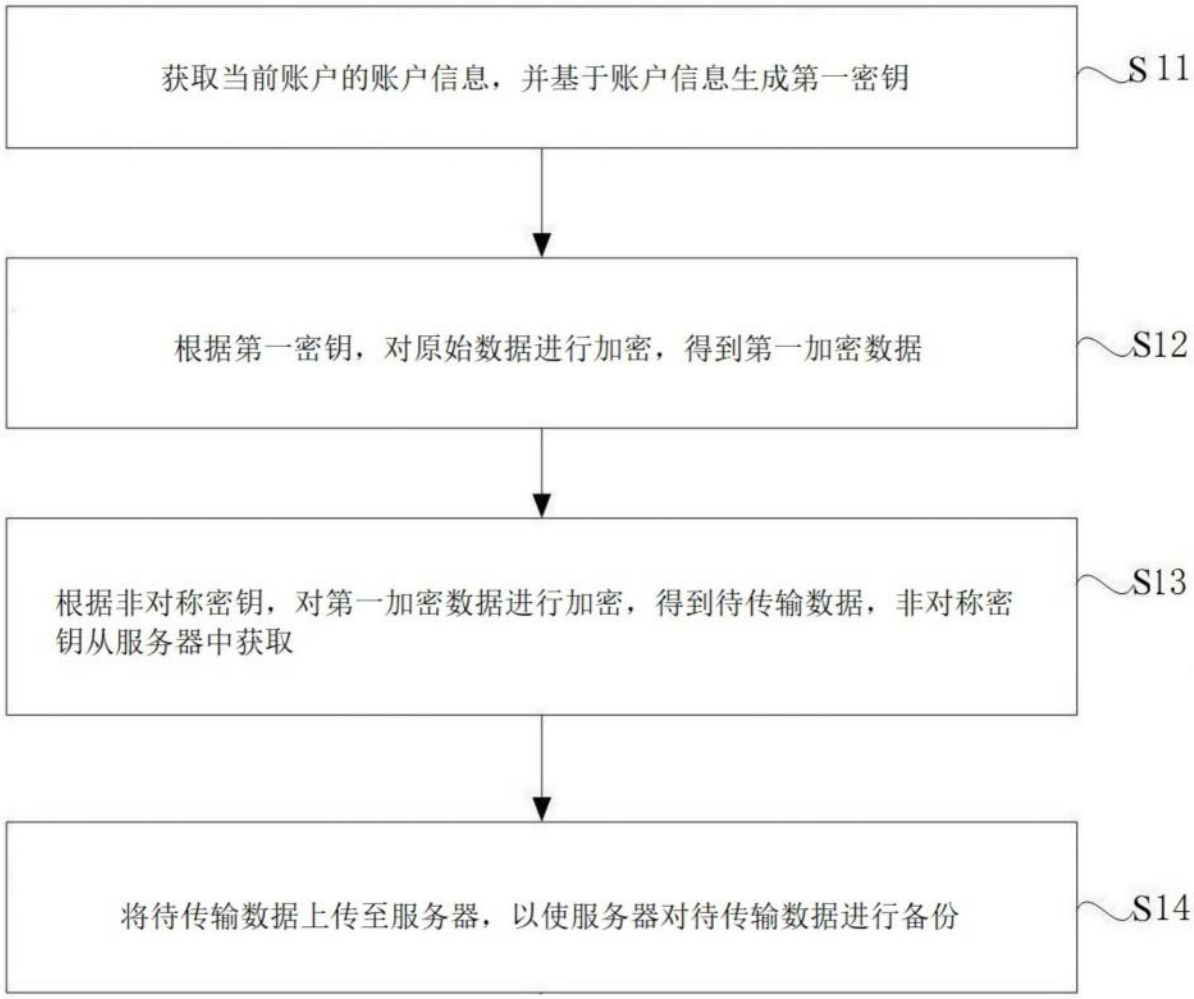

获取当前账户的账户信息，并基于账户信息生成第一密钥
S11
根据第一密钥，对原始数据进行加密，得到第一加密数据
S12
根据非对称密钥，对第一加密数据进行加密，得到待传输数据，非对称密钥从服务器中获取
S13
将待传输数据上传至服务器，以使服务器对待传输数据进行备份
S14

图1

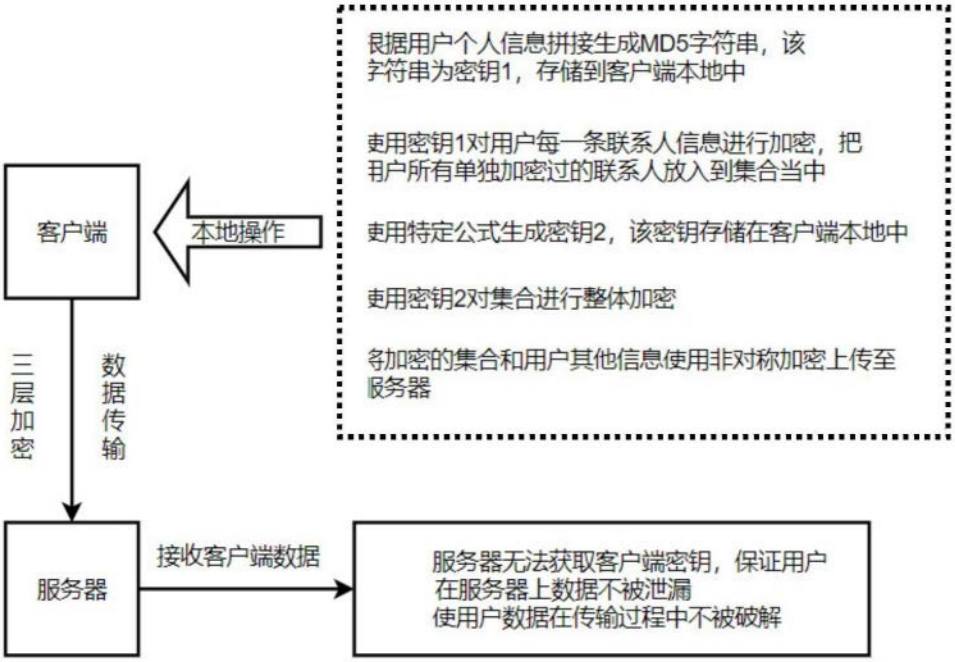

根据用户个人信息拼接生成MD5字符串，该
字符串为密钥1，存储到客户端本地中
使用密钥1对用户每一条联系人信息进行加密，把
用户所有单独加密过的联系人放入到集合当中
使用特定公式生成密钥2，该密钥存储在客户端本地中
使用密钥2对集合进行整体加密
对加密的集合和用户其他信息使用非对称加密上传至
服务器
客户端
本地操作
三层加密
数据传输
服务器
接收客户端数据
服务器无法获取客户端密钥，保证用户
在服务器上数据不被泄漏
使用户数据在传输过程中不被破解

图2


获取单元
201
第一加密单元
202
非对称加密单元
203
传输单元
204

图3

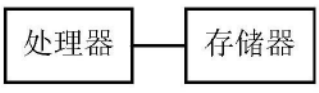

处理器
存储器

图4

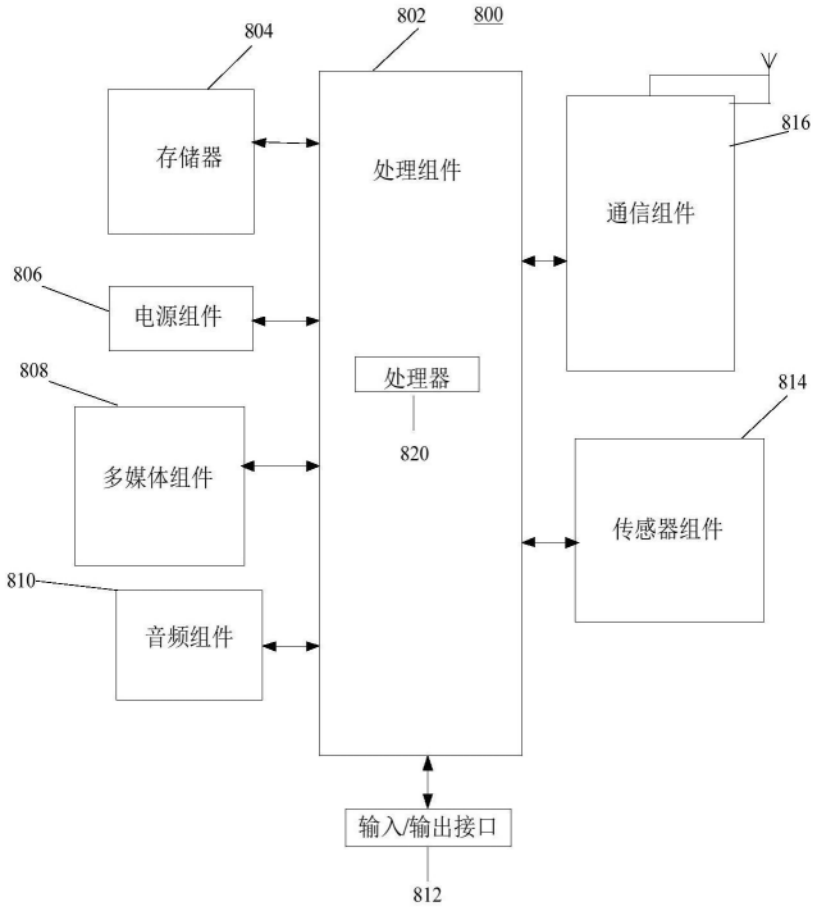

804
802
800
存储器
处理组件
816
通信组件
806
电源组件
处理器
820
808
多媒体组件
814
传感器组件
810
音频组件
输入/输出接口
812

图5