

传输消息的方法、装置、存储介质及电子设备

本公开要求于 2022 年 03 月 29 日提交中国专利局、申请号为 202210324115.0、申请名称为“传输消息的方法、装置、存储介质及电子设备”的中国专利申请的优先权，其全部内容通过引用结合在本公开中。

5

技术领域

本公开涉及云服务访问的领域，具体地，涉及一种传输消息的方法、装置、存储介质及电子设备。

10 背景技术

云服务厂商提供了一系列的服务能力，开发者可以通过厂商提供的应用程序接口（Application Programming Interface，API）来使用和管理这些能力，在调用 API 的过程中，需要使用厂商提供的接口访问密钥对发出的业务请求进行签名，签名的算法通常是开放的，用户只需要获取到账号的密钥就可以对该业务请求进行签名，实现相关功能的接口调用。

15

实际应用场景中，当有多个用户使用同一个云服务时，为了对资源的权限进行控制，一般会独立配置多个不同权限的账号，每个账号访问自己所需要的资源，但由于用户直接访问的是云服务厂商的接口，管理部门无法对各个用户的云服务访问请求进行审计和检测，导致云服务数据访问存在安全风险的问题。

20 发明内容

提供该部分内容以便以简要的形式介绍构思，这些构思将在后面的具体实施方式部分被详细描述。该部分内容并不旨在标识要求保护的技术方案的关键特征或必要特征，也不旨在用于限制所要求的保护的技术方案的范围。

25

第一方面，本公开提供一种传输消息的方法，应用于预设服务器，所述预设服务器为预先部署的在终端和云服务器之间传输消息的服务器，所述方法包括：

接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

30

根据所述云服务访问请求消息确定待访问的云服务接口地址；  
根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；

根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。

35

第二方面，提供一种传输消息的方法，应用于终端，所述方法包括：  
获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；  
根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

将所述云服务访问请求消息发送至所述预设服务器，以便所述预设服务器在对所述云服务访问请求消息进行签名验证并验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

第三方面，提供一种传输消息的装置，应用于预设服务器，所述预设服务器为预先部署的在终端和云服务器之间传输消息的服务器，所述装置包括：

第一接收模块，用于接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

确定模块，用于根据所述云服务访问请求消息确定待访问的云服务接口地址；

验证模块，用于根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；

第一发送模块，用于根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。

第四方面，提供一种传输消息的装置，应用于终端，所述装置包括：

获取模块，用于获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；

请求消息生成模块，用于根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

第二发送模块，用于将所述云服务访问请求消息发送至所述预设服务器，以便所述预设服务器在对所述云服务访问请求消息进行签名验证并验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

第五方面，提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理装置执行时实现本公开第一方面或第二方面所述方法的步骤。

第六方面，提供一种电子设备，包括：存储装置，其上存储有至少一个计算机程序；至少一个处理装置，用于执行所述存储装置中的所述至少一个计算机程序，以实现本公开第一方面或第二方面所述方法的步骤。

第七方面，提供一种计算机程序产品，包括计算机指令，该计算机指令被处理装置执行时实现本公开第一方面或第二方面所述方法的步骤。

第八方面，提供一种计算机程序，该计算机程序被处理装置执行时实现本公开第一方面或第二方面所述方法的步骤。

本公开的其他特征和优点将在随后的具体实施方式部分予以详细说明。

附图说明

结合附图并参考以下具体实施方式，本公开各实施例的上述和其他特征、优点及方面将变得更加明显。贯穿附图中，相同或相似的附图标记表示相同或相似的元素。应当理解附图是示意性的，元件和元素不一定按照比例绘制。在附图中：

图 1 是一种现有的云服务访问模式下的消息传输示意图；

- 图 2 是一种现有的云服务访问模式下的账号分配示意图；  
图 3 是根据一示例性实施例示出的一种传输消息的方法的流程图；  
图 4 是一种现有的云服务访问模式下的消息传输示意图；  
图 5 是根据一示例性实施例示出的一种传输消息的过程示意图；  
5 图 6 是根据一示例性实施例示出的一种传输消息的方法的流程图；  
图 7 是根据一示例性实施例示出的一种传输消息的方法的流程图；  
图 8 是根据一示例性实施例示出的一种传输消息的方法的流程图；  
图 9 是根据一示例性实施例示出的一种传输消息的方法的流程图；  
图 10 是根据一示例性实施例示出的一种传输消息的过程示意图；  
10 图 11 是基于定制化 SDK 的消息传输示意图；  
图 12 是根据一示例性实施例示出的一种传输消息的装置的框图；  
图 13 是根据一示例性实施例示出的一种传输消息的装置的框图；  
图 14 是根据一示例性实施例示出的一种传输消息的装置的框图；  
图 15 是根据一示例性实施例示出的一种电子设备的结构框图。

15

具体实施方式

下面将参照附图更详细地描述本公开的实施例。虽然附图中显示了本公开的某些实施例，然而应当理解的是，本公开可以通过各种形式来实现，而且不应该被解释为限于这里阐述的实施例，相反提供这些实施例是为了更加透彻和完整地理解本公开。应当理解的是，本公开的附图及实施例仅用于示例性作用，并非用于限制本公开的保护范围。

应当理解，本公开的方法实施方式中记载的各个步骤可以按照不同的顺序执行，和/或并行执行。此外，方法实施方式可以包括附加的步骤和/或省略执行示出的步骤。本公开的范围在此方面不受限制。

本文使用的术语“包括”及其变形是开放性包括，即“包括但不限于”。术语“基于”是“至少部分地基于”。术语“一个实施例”表示“至少一个实施例”；术语“另一实施例”表示“至少一个另外的实施例”；术语“一些实施例”表示“至少一些实施例”。其他术语的相关定义将在下文描述中给出。

需要注意，本公开中提及的“第一”、“第二”等概念仅用于对不同的装置、模块或单元进行区分，并非用于限定这些装置、模块或单元所执行的功能的顺序或者相互依存关系。

30 需要注意，本公开中提及的“一个”、“多个”的修饰是示意性而非限制性的，本领域技术人员应当理解，除非在上下文另有明确指出，否则应该理解为“一个或多个”。

本公开实施方式中的多个装置之间所交互的消息或者信息的名称仅用于说明性的目的，而并不是用于对这些消息或信息的范围进行限制。

35 本公开中所有获取信号、信息或数据的动作都是在遵照所在地国家相应的数据保护法规政策的前提下，并获得由相应装置所有者给予授权的情况下进行的。

可以理解的是，在使用本公开各实施例公开的技术方案之前，均应当依据相关法律法规通过恰当的方式对本公开所涉及个人信息的类型、使用范围、使用场景等告知用户并获得用户的授权。

例如，在响应于接收到用户的主动请求时，向用户发送提示信息，以明确地提示用户，其请求执行的操作将需要获取和使用到用户的个人信息。从而，使得用户可以根据提示信息来自主地选择是否向执行本公开技术方案的操作的电子设备、应用程序、服务器或存储介质等软件或硬件提供个人信息。

- 5       作为一种可选的但非限定性的实现方式，响应于接收到用户的主动请求，向用户发送提示信息的方式例如可以是弹窗的方式，弹窗中可以以文字的方式呈现提示信息。此外，弹窗中还可以承载供用户选择“同意”或者“不同意”向电子设备提供个人信息的选择控件。

可以理解的是，上述通知和获取用户授权过程仅是示意性的，不对本公开的实现方式构成限定，其它满足相关法律法规的方式也可应用于本公开的实现方式中。

- 10       同时，可以理解的是，本技术方案所涉及的数据（包括但不限于数据本身、数据的获取或使用）应当遵循相应法律法规及相关规定的要求。

- 本公开主要应用于通过调用云厂商提供的 API 来访问和使用云服务资源的场景中，如图 1 所示，在使用接口时，需要使用厂商提供的接口访问密钥对发出的原始请求进行签名，然后直接将签名请求发送至云服务器，签名的算法通常是开放的，用户只需要获取到账号的密钥  
15       就可以对云服务访问请求进行签名，实现相关功能的接口调用，但由于用户直接访问的是云服务厂商的接口，管理部门无法对各个用户的云服务访问请求进行审计和检测，导致云服务数据访问存在安全风险的问题。

- 如图 2 所示，实际应用场景中，当有多个用户使用同一个云服务时，为了对资源的权限进行控制，一般会独立配置多个不同权限的账号，每个账号访问自己所需要的资源，并且同一用户若需要访问多个云厂商提供的云服务，还需要分别针对每个厂商配置不同的账号，但是，厂商账号会有泄露的风险（比如拥有该账号的用户离职，或者该账号丢失等情况），若某一用户的云服务厂商账号泄露，需要到不同云厂商的管理平台上进行删除操作，另一种可能的场景中，若对某一用户的云服务访问权限进行调整，也需要登录各个云厂商平台进行操作，因此，现有技术中无论是账号泄露还是权限调整，其账号的维护管理均比较困难。

- 20       为解决上述存在的问题，本公开提供一种传输消息的方法、装置、存储介质和电子设备，在终端和云服务器之间预先部署用于传输消息的预设服务器，在终端侧调整云厂商接口访问地址（即在原有的接口访问地址中加入预先为预设服务器配置的预设域名后缀后得到域名地址信息），并使用预设服务器提供的访问密钥对云服务访问请求消息进行签名后，可以将终端发送的云服务访问请求消息引流至预设服务器，由该预设服务器对当前要访问云服务器的用户进行统一的账号验证，也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测，对用户使用的功能、频次等进行统一检测管理，实现了云服务访问的可控性，降低了云服务数据访问的安全风险。

- 通过上述技术方案，预先部署在终端和云服务器之间用于传输消息的预设服务器可以接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；根据所述云服务访问请求消息确定待访问的云服务接口地址；根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器，这样，可以根据该域名地址信息将终端发送的云服务访问请求消息引流至预设服务器，由该预设服务器对当前要访问云服务器的用  
35

户进行统一的账号验证，也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测，实现了云服务访问的可控性，降低了云服务数据访问的安全风险。

另外，基于预设服务器对各个用户的云服务访问请求消息进行统一检测和管理，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门可以通过该预设服务器删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而大大降低了账号的维护管理成本，与此同时，不需要在云厂商中为每个用户单独配置账号，多个用户可以共用一个真实密钥，只需要为每个用户分配一个伪签名密钥即可达到账号隔离的效果，当发生单个用户账号的泄露时不会影响其他用户。

下面结合附图对本公开的具体实施方式进行详细说明。

图 3 是根据一示例性实施例示出的一种传输消息的方法的流程图，该方法应用于预设服务器，该预设服务器为预先部署的在终端和云服务器之间传输消息的服务器，该预设服务器可以理解为是在终端和服务端之间预设的中间代理服务，如图 3 所示，该方法包括以下步骤：

在步骤 S301 中，接收该终端发送的云服务访问请求消息，该云服务访问请求消息中包括该预设服务器的域名地址信息。

其中，该云服务访问请求消息包括要访问云服务的当前用户（例如，需要使用云服务资源的开发者）的用户标识信息、具体的业务请求数据以及该预设服务器的域名地址信息，其中，该域名地址信息中包括当前用户待访问的云服务器对应的云厂商的云服务接口地址和该预设服务器对应的预设域名后缀，通过在该云服务接口地址后加入该预设域名后缀，可以将该云服务访问请求消息引流至该预设服务器，以便通过该预设服务器对当前要访问云服务器的用户进行统一的账号验证，也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测。

在步骤 S302 中，根据该云服务访问请求消息确定待访问的云服务接口地址。

在本步骤中，可以获取该预设服务器对应的预设域名后缀；从该云服务访问请求消息中获取域名地址信息；这样，可以根据该预设域名后缀从该域名地址信息中确定该云服务接口地址。

上述已经提及，为了将该云服务访问请求消息引流至该预设服务器，可以预先为该预设服务器配置一个预设域名后缀（即该预设域名后缀），之后可以在云服务接口地址中添加该预设域名后缀，得到该域名地址信息，这样，在根据该预设域名后缀从该域名地址信息中确定该云服务接口地址的过程中，可以将该域名地址信息中的预设域名后缀删除后还原出原有的云服务接口地址。

示例地，图 4 是现有技术中访问云服务时的访问模式示意图，在原有的模式下，用户可以直接使用云厂商的接口访问地址和密钥访问接口服务，如图 4 所示，客户端直接可以使用 A 厂商的云服务接口地址 `api.a.com` 访问 A 厂商接口，直接可以使用 B 厂商的云服务接口地址 `api.b.com` 访问 B 厂商接口，直接可以使用 C 厂商的云服务接口地址 `api.c.com` 访问 C 厂商接口，在本公开中，如图 5 所示，为了将该云服务访问请求消息引流至该预设服务器（即图 5 中的中间代理），可以预先为该预设服务器配置一个泛域名 `*.fusion-api.com`，这样，可以在原有的云服务接口地址中添加预设域名后缀 `.fusion-api.com`，就能够完成请求的引流，该预设服务器在接收到请求消息后，可以将请求消息中该域名地址信息中的预设域名后缀删除后还原出原有的云服务接口地址，如图 5 所示，预设服务器接收到的访问 A 厂商的云服务访问请求

消息中的域名地址信息为 api.a.com.fusion-api.com，对该请求消息进行还原后，可以得到 A 厂商原始的云服务接口地址为 api.a.com，上述示例仅是举例说明，本公开对此不作限定。

实际应用场景中，为了对资源的访问权限进行控制，预设服务器可以预先为不同的用户访问不同的接口分别配置不同的账号（即 Access Key Id，AK），当前用户的用户标识信息包括该 AK 账号，不同的用户标识信息对应不同的云服务接口，因此，在本步骤另一种可能的实现方式中，还可以根据该云服务访问请求消息中的用户标识信息确定该云服务接口地址，例如，预设服务器可以预先在数据库中存储 AK 账号与云服务接口的对应关系，服务器在接收到该云服务访问请求消息后，可以从该云服务访问请求消息中的用户标识信息中读取到 AK 账号，之后可以通过查表的方式获取到当前用户待访问的云服务接口，进而确定出该云服务接口地址。

在步骤 S303 中，根据该云服务接口地址对该云服务访问请求消息进行签名验证，并在验证通过的情况下，对该云服务访问请求消息进行重新签名，得到新的云服务访问请求消息。

其中，该云服务访问请求消息包括当前用户的用户标识信息和业务请求数据，该业务请求数据包括该当前用户待访问的云服务器的对应的云厂商的厂商标识信息。

图 6 是根据一示例性实施例示出的一种传输消息的方法的流程图，如图 6 所示，可以通过执行以下步骤根据该云服务接口地址对该云服务访问请求消息进行签名验证：

在步骤 S3031 中，根据该云服务接口地址确定该云服务器对应的签名算法。

实际应用场景中，不同的云厂商对应不同的签名算法，并且每个云厂商均对外公开该签名算法，本步骤中，可以根据该云服务接口地址确定当前待访问的云服务器对应的云厂商，进而可以确定出该云厂商对应的签名算法。

在步骤 S3032 中，根据该用户标识信息和该厂商标识信息获取当前用户对应的第一密钥，该第一密钥为该预设服务器预先生成的。

相比较于云服务器对应的真实密钥，该第一密钥可以理解为是由预设服务器为用户生成的伪密钥。

在一种可能的应用场景中，可以在预设服务器中预先存储用户、云厂商和该伪密钥的对应关系，这样，在本步骤中可以根据该用户标识信息和该厂商标识信息通过查表的方式获取到该第一密钥。

示例地，表 1 是预设服务器中存储的用户信息、厂商信息以及对应的密钥信息的对应关系，如表 1 所示，假设当前用户为用户 u1，用户 u1 想要访问云厂商 A 提供的云服务资源，此种情况下，预设服务器可以从云服务访问请求消息中获取到用户标识信息 u1 和厂商标识信息 A，之后可以通过查表 1，确定出用户 u1 以及云厂商 A 对应的第一密钥即为 FakeKey1，上述示例仅是举例说明，本公开对此不作限定。

| 用户 | 云厂商 | 伪密钥      | 真实密钥     |
|----|-----|----------|----------|
| u1 | A   | FakeKey1 | RealKey1 |
| u2 | B   | FakeKey2 | RealKey2 |
| u3 | C   | FakeKey3 | RealKey3 |
| u4 | D   | FakeKey4 | RealKey4 |

表 1

在步骤 S3033 中, 根据该第一密钥、该用户标识信息以及该业务请求数据采用该签名算法生成第一签名。

本步骤可以根据该用户标识信息、该业务请求数据以及该第一密钥基于该签名算法重新计算得到该第一签名, 具体的计算方式可以参考相关文献中的描述, 在此不作限定。

5 在步骤 S3034 中, 根据该第一签名对该云服务访问请求消息进行签名验证。

一种可能的实现方式中, 可以将该第一签名与该云服务访问请求消息中的签名信息进行比对, 若两者完全一致, 确定该云服务访问请求消息验证通过, 之后, 即可对该云服务访问请求消息进行密钥替换, 并将采用云服务器提供的真实密钥签名的请求消息发送至云服务器, 以便实现对云服务器接口的调用。

10 在步骤 S3035 中, 根据该用户标识信息和该厂商标识信息获取该云服务器对应的第二密钥, 该第二密钥为该云服务器预先生成的。

其中, 该第二密钥即为云服务器提供的真实密钥。

在本步骤中, 预设服务器也可以通过查表的方式根据该用户标识信息和该厂商标识信息查找到对应的该第二密钥。

15 示例地, 继续以表 1 为例, 假设当前用户为用户 u1, 用户 u1 想要访问云厂商 A 提供的云服务资源, 此种情况下, 预设服务器可以从云服务访问请求消息中获取到用户标识信息 u1 和厂商标识信息 A, 之后可以通过查表 1, 确定出用户 u1 以及云厂商 A 对应的第二密钥即为 RealKey1, 上述示例仅是举例说明, 本公开对此不作限定。

20 在步骤 S3036 中, 根据该第二密钥、该用户标识信息以及该业务请求数据采用该签名算法生成第二签名。

同样地, 本步骤可以根据第二密钥、该用户标识信息以及该业务请求数据基于该签名算法重新计算得到该第二签名。

在步骤 S3037 中, 根据该第二签名对该云服务访问请求消息进行重新签名, 得到该新的云服务访问请求消息。

25 在一种可能的实现方式中, 可以将云服务访问请求消息中的原始签名替换为该第二签名, 以实现根据该第二签名对该云服务访问请求消息进行重新签名, 得到该新的云服务访问请求消息, 其中, 该原始签名即为终端采用预设服务器分配的伪密钥生成的签名。

30 基于图 6 所示的步骤, 预设服务器可以对终端发送的采用伪密钥签名的云服务访问请求消息进行签名验证, 并在验证通过的情况下, 可以采用云服务器提供的真实密钥对该云服务访问请求消息进行重新签名, 这样不仅可以实现对云服务访问账号的统一管理, 还能对各个用户的云服务访问请求进行审计和检测, 例如, 可以及时掌握用户访问了哪些资源, 用了哪些云服务接口功能, 云厂商对当前用户请求的处理服务能力质量如何等 (比如响应速度), 遇到了哪些问题等, 进而可以评估用户使用的资源数据是否安全, 也可以对云厂商的服务能力进行评估。

35 在步骤 S304 中, 根据该云服务接口地址将该新的云服务访问请求消息发送至该云服务器。

采用上述方法, 可以根据该域名地址信息将终端发送的云服务访问请求消息引流至预设服务器, 由该预设服务器对当前要访问云服务器的用户进行统一的账号验证, 也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测, 实现了云服务访问的可控性, 降低了云服务数据访问的安全风险。

另外，基于预设服务器对各个用户的云服务访问请求消息进行统一检测和管理，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门可以通过该预设服务器删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而大大降低了账号的维护管理成本，与此同时，不需要在云厂商中为每个用户单独配置账号，多个用户可以共用一个真实密钥，只需要为每个用户分配一个伪签名密钥即可达到账号隔离的效果，当发生单个用户账号的泄露时不会影响其他用户。

图 7 是根据图 3 所示实施例示出的一种传输消息的方法的流程图，如图 7 所示，该方法还包括：

- 10 在步骤 S305 中，接收该云服务器根据该新的云服务访问请求消息发送的云服务访问响应消息，并将该云服务访问响应消息发送至该终端。

其中，该云服务访问响应消息可以包括业务响应信息，预设服务器在将重新签名后的新的云服务访问请求消息发送至云服务器后，可以接收到云服务器返回的该云服务访问响应消息，之后可以将该云服务访问响应消息发送至该终端。

如图 7 所示，该方法还包括以下步骤：

- 15 在步骤 S306 中，根据该新的云服务访问请求消息和该云服务访问响应消息生成访问日志。

其中，该访问日志用于记录当前用户的云服务访问事项，该云服务访问事项包括当前用户访问的目标资源，当前用户使用的目标接口功能，云厂商对当前用户请求的处理服务能力质量（如响应速度），当前访问是否遇到问题以及遇到何种问题，评估当前用户使用的资源数据是否安全等事项。

- 20 在本步骤中，可以根据该新的云服务访问请求消息、云服务访问响应消息以及请求消息发送时间，响应消息的接收时间等生成该访问日志，以实现当前用户的云服务访问请求进行审计和检测。

图 8 是根据一示例性实施例示出的一种传输消息的方法的流程图，该方法可以应用于终端，如图 8 所示，该方法包括以下步骤：

- 25 在步骤 S801 中，获取当前用户的用户标识信息、业务请求数据以及预设服务器为该当前用户预先分配的访问密钥。

- 30 其中，该业务请求数据可以包括当前用户待访问的云服务器的对应的云厂商的厂商标识信息、实际的业务访问参数等信息，该预设服务器为预先部署的在该终端和云服务器之间传输消息的服务器，该预设服务器可以理解为是终端和服务器之间预设的中间代理服务，相较于原有的云服务访问模式下，云服务器为用户分配的真实密钥，该访问密钥是指由该预设服务器为用户预先分配的伪密钥。

在步骤 S802 中，根据该用户标识信息、该业务请求数据以及该访问密钥生成云服务访问请求消息，该云服务访问请求消息中包括该预设服务器的域名地址信息。

- 35 在本步骤中，可以根据该业务请求数据中的厂商标识信息获取该云服务器的云服务接口地址；根据该云服务接口地址和该预设服务器对应的预设域名后缀生成域名地址信息；根据该访问密钥、该用户标识信息以及该业务请求数据采用该云服务器提供的签名算法生成第三签名；根据该第三签名、该用户标识信息、该业务请求数据以及该域名地址信息生成该云服务访问请求消息。

本公开中为了通过该预设服务器对用户发送的云服务访问请求进行统一的检测和管理，需要将该云服务访问请求消息引流至该预设服务器，在一种可能的实现方式中，可以预先为该预设服务器配置一个泛域名，终端可以根据该泛域名调整每个云厂商的云服务接口地址，例如，A 厂商的云服务接口地址为 api.a.com，可以再改地址后添加一个预设域名后缀.fusion-api.com 后生成域名地址信息，这样，终端可以根据该域名地址信息将该云服务访问请求消息发送至该预设服务器，从而实现请求消息的引流。

需要说明的是，可以预先设置该预设域名后缀与该预设服务器 IP 地址的对应关系，这样可以保证发送至该预设域名后缀对应的地址上的消息均可以引流至该预设服务器。

在生成该域名地址信息后，即可根据该访问密钥、该用户标识信息以及该业务请求数据采用该云服务器提供的签名算法计算得到该第三签名，具体生成该第三签名的过程可以参考相关文献中的描述，在此不作限定，在生成该第三签名后，即可根据该第三签名、该用户标识信息、该业务请求数据以及该域名地址信息生成该云服务访问请求消息。

在步骤 S803 中，将该云服务访问请求消息发送至该预设服务器。

这样该预设服务器在对该云服务访问请求消息进行签名验证通过的情况下，可以对该云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将该新的云服务访问请求消息发送至该云服务器。

采用上述方法，终端可以通过调整云厂商的云服务接口地址，在该云服务接口地址后加入该预设服务器对应的预设域名后缀后，将终端发送的云服务访问请求消息发送至预设服务器，由该预设服务器对当前要访问云服务器的用户进行统一的账号验证，也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测，实现了云服务访问的可控性，降低了云服务数据访问的安全风险。

另外，基于预设服务器对各个用户的云服务访问请求消息进行统一检测和管理，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门可以通过该预设服务器删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而大大降低了账号的维护管理成本，与此同时，不需要在云厂商中为每个用户单独配置账号，多个用户可以共用一个真实密钥，只需要为每个用户分配一个伪签名密钥即可达到账号隔离的效果，当发生单个用户账号的泄露时不会影响其他用户。

图 9 是根据一示例性实施例示出的一种传输消息的方法的流程图，如图 9 所示，该方法包括以下步骤：

在步骤 S901 中，终端获取当前用户的用户标识信息、业务请求数据以及预设服务器为该当前用户预先分配的访问密钥。

其中，该当前用户一般是指当前时刻需要使用云服务资源的开发者，该业务请求数据可以包括当前用户待访问的云服务器的对应的云厂商的厂商标识信息、实际的业务访问参数等信息，该预设服务器为预先部署的在该终端和云服务器之间传输消息的服务器，该预设服务器可以理解为是终端和服务器之间预设的中间代理服务，相比较于原有的云服务访问模式下，云服务器为用户分配的真实密钥，该访问密钥是指由该预设服务器为用户预先分配的伪密钥。

在步骤 S902 中，终端根据该用户标识信息、该业务请求数据以及该访问密钥生成云服务访问请求消息，该云服务访问请求消息中包括该预设服务器的域名地址信息。

其中，该业务请求数据包括该当前用户待访问的该云服务器的对应的云厂商的厂商标识信息，在本步骤中，终端可以根据该厂商标识信息获取该云服务器的云服务接口地址；根据该云服务接口地址和该预设服务器对应的预设域名后缀生成域名地址信息；根据该访问密钥、该用户标识信息以及该业务请求数据采用该云服务器提供的签名算法生成第三签名；根据该第三签名、该用户标识信息、该业务请求数据以及该域名地址信息生成该云服务访问请求消息。

在本公开中，为了通过该预设服务器对用户发送的云服务访问请求进行统一的检测和管理，需要将该云服务访问请求消息引流至该预设服务器，在一种可能的实现方式中，可以预先为该预设服务器配置一个泛域名，终端可以根据该泛域名调整每个云厂商的云服务接口地址，例如，A 厂商的云服务接口地址为 `api.a.com`，可以再改地址后添加一个预设域名后缀 `.fusion-api.com` 后生成域名地址信息，这样，终端可以根据该域名地址信息将该云服务访问请求消息发送至该预设服务器，从而实现请求消息的引流。

需要说明的是，可以预先设置该预设域名后缀与该预设服务器 IP 地址的对应关系，这样可以保证发送至该预设域名后缀对应的地址上的消息均可以引流至该预设服务器。

在步骤 S903 中，终端将该云服务访问请求消息发送至该预设服务器。

在步骤 S904 中，预设服务器根据该云服务访问请求消息确定待访问的云服务接口地址。在本步骤中，可以获取该预设服务器对应的预设域名后缀，并从该云服务访问请求消息中获取域名地址信息，根据该预设域名后缀从该域名地址信息中确定该云服务接口地址，具体示例可以参考图 3 对应的实施例中的描述，在此不再赘述。

在另一种可能的实现方式中，不同的用户标识信息可以对应不同的云服务接口，因此本步骤还可以根据该云服务访问请求消息中的用户标识信息确定该云服务接口地址，例如，预设服务器可以预先在数据库中存储 AK 账号与云服务接口的对应关系，服务器在接收到该云服务访问请求消息后，可以从该云服务访问请求消息中的用户标识信息中读取到 AK 账号，之后可以通过查表的方式获取到当前用户待访问的云服务接口，进而确定出该云服务接口地址。

在步骤 S905 中，预设服务器根据该云服务接口地址对该云服务访问请求消息进行签名验证，并在验证通过的情况下，对该云服务访问请求消息进行重新签名，得到新的云服务访问请求消息。

其中，该云服务访问请求消息包括当前用户的用户标识信息和业务请求数据，该业务请求数据包括该当前用户待访问的云服务器的对应的云厂商的厂商标识信息。

在本步骤中，可以根据该云服务接口地址确定该云服务器对应的签名算法；根据该用户标识信息和该厂商标识信息获取当前用户对应的第一密钥，该第一密钥为该预设服务器预先生成的；根据该第一密钥、该用户标识信息以及该业务请求数据采用该签名算法生成第一签名；根据该第一签名对该云服务访问请求消息进行签名验证。

之后，可以根据该用户标识信息和该厂商标识信息获取该云服务器对应的第二密钥，该第二密钥为该云服务器预先生成的；根据该第二密钥、该用户标识信息以及该业务请求数据采用该签名算法生成第二签名；根据该第二签名对该云服务访问请求消息进行重新签名，得到该新的云服务访问请求消息。

其中，该相比较于云服务器对应的真实密钥，该第一密钥可以理解为是由预设服务器为用户生成的伪密钥，该第二密钥即为云服务器提供的真实密钥。

本步骤的具体实现方式也可以参考图 6 对应的实施例中的相关描述，在此不再赘述。

在步骤 S906 中，预设服务器根据该云服务接口地址将该新的云服务访问请求消息发送至该云服务器。

在步骤 S907 中，预设服务器接收该云服务器根据该新的云服务访问请求消息发送的云服务访问响应消息，并将该云服务访问响应消息发送至该终端。

其中，该云服务访问响应消息可以包括业务响应信息，预设服务器在将重新签名后的新的云服务访问请求消息发送至云服务器后，可以接收到云服务器返回的该云服务访问响应消息，之后可以将该云服务访问响应消息发送至该终端。

在步骤 S908 中，预设服务器根据该新的云服务访问请求消息和该云服务访问响应消息生成访问日志，该访问日志用于记录当前用户的云服务访问事项。

其中，该访问日志用于记录当前用户的云服务访问事项，该云服务访问事项包括当前用户访问的目标资源，当前用户使用的目标接口功能，云厂商对当前用户请求的处理服务能力质量（如响应速度），当前访问是否遇到问题以及遇到何种问题，评估当前用户使用的资源数据是否安全等事项。

在本步骤中，可以根据该新的云服务访问请求消息、云服务访问响应消息以及请求消息发送时间，响应消息的接收时间等生成该访问日志，以实现当前用户的云服务访问请求进行审计和检测。

示例地，图 10 是根据一示例性实施例示出的一种在终端、预设服务器（即图 10 中的中间代理）和云服务器之间传输消息的过程示意图，终端侧先使用预设服务器分配的伪密钥（即第一密钥）对原始的云服务访问请求消息进行签名，如图 10 所示，用户 u1 想要访问 A 厂商提供的云服务，在终端侧基于预设服务器分配的伪密钥对请求消息进行签名后得到的云服务访问请求消息为“vendor=A,user=u1,sign=signA(u1,FakeKey1)”，终端将该云服务访问请求消息发送至预设服务器，预设服务器在表 1 中查表获取到用户 u1 和厂商 A 对应的伪密钥为 FakeKey1，基于该伪密钥 FakeKey1 和厂商 A 提供的签名算法重新生成签名后对请求消息“vendor=A,user=u1,sign=signA(u1,FakeKey1)”进行签名验证，在验证通过后，根据用户 u1 和厂商 A 继续查表 1 获取到厂商 A 为用户 u1 分配的真实密钥 RealKey1，然后根据该真实密钥 RealKey1 采用厂商 A 提供的签名算法重新生成签名后，将请求消息进行密钥替换后，得到新的云服务访问请求消息为“vendor=A,user=u1,sign=signA(u1,RealKey1)”，然后预设服务器将该新的云服务访问请求消息发送至 A 厂商对应的云服务器，以实现 A 厂商提供的云服务的资源访问，上述示例仅是举例说明，本公开对此不作限定。

采用上述方法，可以根据云服务访问请求消息中的域名地址信息将终端发送的云服务访问请求消息引流至预设服务器，由该预设服务器对当前要访问云服务器的用户进行统一的账号验证，也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测，实现了云服务访问的可控性，降低了云服务数据访问的安全风险。

基于预设服务器对各个用户的云服务访问请求消息进行统一检测和管理，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门可以通过该预设服务器删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而大大降低

了账号的维护管理成本，与此同时，不需要在云厂商中为每个用户单独配置账号，多个用户可以共用一个真实密钥，只需要为每个用户分配一个伪签名密钥即可达到账号隔离的效果，当发生单个用户账号的泄露时不会影响其他用户。

- 5 另外，基于上述的云服务访问模式，用户可以继续使用原有的厂商接口规范和软件开发工具包（Software Development Kit，SDK），只需要在终端侧的 SDK 中在待访问的云厂商的接口访问地址后添加预设服务器对应的预设域名后缀即可，用户使用较方便，并且现有的云厂商的功能接口可以直接支持，通用型强，实现成本较低。

- 10 为了解决现有技术中在通过调用云厂商提供的 API 来访问和使用云服务资源时，由于用户直接访问的是云服务厂商的接口，管理部门无法对各个用户的云服务访问请求进行审计和检测，导致云服务数据访问存在安全风险的问题，本公开还可以通过开发统一网关的方式将所有的用户的云服务访问请求统一对接网关服务。

- 15 在一种可能的实现方式中，终端可以向网关发送第一请求消息，该第一请求消息用于请求从网关获取云服务资源信息，其中，终端可以使用网关提供的密钥以及网关提供的签名算法对该第一请求消息进行签名，网关在接收到该第一请求消息后，对该第一请求消息进行签名验证，并在验证通过的情况下，可以采用云厂商提供的密钥和签名算法对该第一请求消息进行重新签名后得到第二请求消息，然后将该第二请求消息发送至云服务器。

- 20 采用统一对接网关服务的方式，管理部门也可以通过该网关服务对用户的云服务访问请求进行审计和检测，实现了云服务访问的可控性，降低云服务数据访问的安全风险，与此同时，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门也可以通过该网关服务删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而降低了账号的维护管理成本，另外，不需要在云厂商中为每个用户单独配置账号，多个用户可以共用一个真实密钥，只需要为每个用户分配一个伪签名密钥即可达到账号隔离的效果，当发生单个用户账号的泄露时不会影响其他用户。

- 25 需要说明的是，用户使用网关服务，由网关服务去调用云厂商的接口，在预先配置该统一网关的过程中，需要对每个云厂商的每一个接口进行适配，但每个云厂商有多个产品，每个产品对应几十个开放接口，也就是说每个厂商一般可能会有上千个接口，统一网关需要将该厂商对应的上千个接口都封装起来，开发成本较高，针对不同的云厂商，对应的接口规范不一样，若在网关侧用一个接口去隐藏全部云厂商对应的接口功能，也会增加开发成本，并且采用这种统一网关，云厂商的 SDK 和文档不再可用，对于用户来说需要额外的学习成本。

- 30 为了解决现有技术中在通过调用云厂商提供的 API 来访问和使用云服务资源时，由于用户直接访问的是云服务厂商的接口，管理部门无法对各个用户的云服务访问请求进行审计和检测，导致云服务数据访问存在安全风险的问题，本公开还可以通过定制化 SDK 的方式进行云服务资源的访问，具体地，可以在终端侧的不同云厂商的 SDK 中添加统一的审计代码，以实现账号的获取以及访问请求的审计。

- 35 图 11 是根据一示例性实施例示出的一种基于定制化 SDK 进行云服务访问的传输消息过程示意图，如图 11 所示，终端可以向审计服务器发送第三请求消息（即图 11 中所示的步骤 1），该第三请求消息用于请求获取待访问的云服务器对应的厂商账号，并请求对该云服务访问请求进行审计，审计服务接收到该第三请求消息后可以对该云服务访问请求进行审计，还可以对该第三请求消息进行签名验证，在验证通过的情况下，可以将当前用户要访问的云服务器

对应的厂商账号发送至终端，之后终端可以采用审计服务发送的厂商账号和密钥信息对访问请求消息进行签名后发送至云服务器（即图 11 中所示的步骤 2）。

因此，采用定制化 SDK 的方式，管理部门也可以通过该审计服务对用户的云服务访问请求进行审计和检测，实现了云服务访问的可控性，降低云服务数据访问的安全风险，与此同时，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门也可以通过该审计服务删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而降低了账号的维护管理成本。

需要说明的是，采用定制化 SDK 的方式，由于用户可能使用的是不同编程语言的 SDK，采用这种方案需要对每个云厂商的每一种语言的 SDK 进行改造，这也会增加开发成本。

10 图 12 是根据一示例性实施例示出的一种传输消息的装置的框图，应用于预设服务器，所述预设服务器为预先部署的在终端和云服务器之间传输消息的服务器，如图 12 所示，所述装置包括：

第一接收模块 1201，用于接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

15 确定模块 1202，用于根据所述云服务访问请求消息确定待访问的云服务接口地址；

验证模块 1203，用于根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；

20 第一发送模块 1204，用于根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。

可选地，所述确定模块 1202，用于获取所述预设服务器对应的预设域名后缀；从所述云服务访问请求消息中获取所述域名地址信息；根据所述预设域名后缀从所述域名地址信息中确定所述云服务接口地址。

25 可选地，所述云服务访问请求消息包括当前用户的用户标识信息和业务请求数据，所述业务请求数据包括所述当前用户待访问的云服务器的对应的云厂商的厂商标识信息，所述验证模块 1203，用于根据所述云服务接口地址确定所述云服务器对应的签名算法；根据所述用户标识信息和所述厂商标识信息获取当前用户对应的第一密钥，所述第一密钥为所述预设服务器预先生成的；根据所述第一密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第一签名；根据所述第一签名对所述云服务访问请求消息进行签名验证。

30 可选地，所述验证模块 1203，用于根据所述用户标识信息和所述厂商标识信息获取所述云服务器对应的第二密钥，所述第二密钥为所述云服务器预先生成的；根据所述第二密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第二签名；根据所述第二签名对所述云服务访问请求消息进行重新签名，得到所述新的云服务访问请求消息。

35 可选地，图 13 是根据图 12 所示实施例示出的一种传输消息的装置的框图，如图 13 所示，该装置还包括：

第二接收模块 1205，用于接收所述云服务器根据所述新的云服务访问请求消息发送的云服务访问响应消息，并将所述云服务访问响应消息发送至所述终端。

可选地，如图 13 所示，该装置还包括：

日志生成模块 1206，用于根据所述新的云服务访问请求消息和所述云服务访问响应消息生成访问日志，所述访问日志用于记录当前用户的云服务访问事项。

采用上述装置，可以将终端发送的云服务访问请求消息引流至预设服务器，由该预设服务器对当前要访问云服务器的用户进行统一的账号验证，也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测，实现了云服务访问的可控性，降低了云服务数据访问的安全风险。

另外，基于预设服务器对各个用户的云服务访问请求消息进行统一检测和管理，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门可以通过该预设服务器删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而大大降低了账号的维护管理成本，与此同时，不需要在云厂商中为每个用户单独配置账号，多个用户可以共用一个真实密钥，只需要为每个用户分配一个伪签名密钥即可达到账号隔离的效果，当发生单个用户账号的泄露时不会影响其他用户。

图 14 是根据一示例性实施例示出的一种传输消息的装置的框图，应用于终端，如图 14 所示，所述装置包括：

获取模块 1401，用于获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；

请求消息生成模块 1402，用于根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

第二发送模块 1403，用于将所述云服务访问请求消息发送至所述预设服务器，以便所述预设服务器在对所述云服务访问请求消息进行签名验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

可选地，所述业务请求数据包括所述当前用户待访问的所述云服务器的对应的云厂商的厂商标识信息，所述请求消息生成模块 1402，用于根据所述厂商标识信息获取所述云服务器的云服务接口地址；根据所述云服务接口地址和所述预设服务器对应的预设域名后缀生成域名地址信息；根据所述访问密钥、所述用户标识信息以及所述业务请求数据采用所述云服务器提供的签名算法生成第三签名；根据所述第三签名、所述用户标识信息、所述业务请求数据以及所述域名地址信息生成所述云服务访问请求消息。

采用上述装置，终端可以通过调整云厂商的云服务接口地址，在该云服务接口地址后加入该预设服务器对应的预设域名后缀后，将终端发送的云服务访问请求消息发送至预设服务器，由该预设服务器对当前要访问云服务器的用户进行统一的账号验证，也使得管理部门可以通过该预设服务器对该云服务访问请求消息进行审计和检测，实现了云服务访问的可控性，降低了云服务数据访问的安全风险。

另外，基于预设服务器对各个用户的云服务访问请求消息进行统一检测和管理，当某一用户对应的账号（一个账号或者多个云厂商对应的多个账号）泄露的情况下，管理部门可以通过该预设服务器删除该用户的账号，无需登录多个云厂商平台分别进行删除操作，从而大大降低了账号的维护管理成本，与此同时，不需要在云厂商中为每个用户单独配置账号，多

个用户可以共用一个真实密钥，只需要为每个用户分配一个伪签名密钥即可达到账号隔离的效果，当发生单个用户账号的泄露时不会影响到其他用户。

下面参考图 15，其示出了适于用来实现本公开实施例的电子设备 1500 的结构示意图。本公开实施例中的终端设备可以包括但不限于诸如移动电话、笔记本电脑、数字广播接收器、  
5 个人数字助理（Personal Digital Assistant, PDA）、平板电脑（Portable Android Device, PAD）、便携式多媒体播放器（Portable Media Player, PMP）、车载终端（例如车载导航终端）等等的移动终端以及诸如数字 TV（Television）、台式计算机等等的固定终端。图 15 示出的电子设备仅仅是一个示例，不对本公开实施例的功能和使用范围带来任何限制。

10 如图 15 所示，电子设备 1500 可以包括处理装置（例如中央处理器、图形处理器等）1501，其可以根据存储在只读存储器（Read Only Memory, ROM）1502 中的程序或者从存储装置 1508 加载到随机访问存储器（Random Access Memory, RAM）1503 中的程序而执行各种适当的动作和处理。在 RAM 1503 中，还存储有电子设备 1500 操作所需的各种程序和数据。处理装置 1501、ROM 1502 以及 RAM 1503 通过总线 1504 彼此相连。输入/输出（Input/Output, I/O）接口 1505 也连接至总线 1504。

15 通常，以下装置可以连接至 I/O 接口 1505：包括例如触摸屏、触摸板、键盘、鼠标、摄像头、麦克风、加速度计、陀螺仪等的输入装置 1506；包括例如液晶显示器（Liquid Crystal Display, LCD）、扬声器、振动器等等的输出装置 1507；包括例如磁带、硬盘等的存储装置 1508；以及通信装置 1509。通信装置 1509 可以允许电子设备 1500 与其他设备进行无线或有线通信以交换数据。虽然图 15 示出了具有各种装置的电子设备 1500，但是应理解的是，并不要求实  
20 施或具备所有示出的装置。可以替代地实施或具备更多或更少的装置。

特别地，根据本公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括承载在非暂态计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信装置 1509 从网络上被下载和安装，或者从存储装置 1508  
25 被安装，或者从 ROM 1502 被安装。在该计算机程序被处理装置 1501 执行时，执行本公开实施例的方法中限定的上述功能。

本公开实施例还提供了一种计算机程序，该计算机程序存储在可读存储介质中，电子设备的一个或多个处理器可以从所述可读存储介质中读取所述计算机程序，所述一个或多个处理器执行所述计算机程序，使得所述电子设备执行上述任一实施例提供的方案。

30 需要说明的是，本公开上述的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器  
35 （Erasable Programmable Read-Only Memory, EPROM 或闪存）、光纤、便携式紧凑磁盘只读存储器（Portable Compact Disk Read-Only Memory, CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。在本公开中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本公开中，计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承

载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读信号介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以

5 用任何适当的介质传输，包括但不限于：电线、光缆、RF（Radio Frequency，射频）等等，或者上述的任意合适的组合。

在一些实施方式中，客户端、服务器可以利用诸如超文本传输协议（HTTP，HyperText Transfer Protocol）之类的任何当前已知或未来研发的网络协议进行通信，并且可以与任意形式或介质的数字数据通信（例如，通信网络）互连。通信网络的示例包括局域网（LAN，Local

10 Area Network），广域网（WAN，Wide Area Network），网际网（例如，互联网）以及端对端网络（例如，ad hoc 端对端网络），以及任何当前已知或未来研发的网络。

上述计算机可读介质可以是上述电子设备中所包含的；也可以是单独存在，而未装配入该电子设备中。

上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被该电子设备

15 执行时，使得该电子设备：接收所述终端发送的云服务访问请求消息；根据所述云服务访问请求消息确定待访问的云服务接口地址；根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。

或者，上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被该电子设备执行时，使得该电子设备：获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息；将所述云服务访问请求消息发送至所述预设服务器，以便所述预

20 设服务器在对所述云服务访问请求消息进行签名验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

可以以一种或多种程序设计语言或其组合来编写用于执行本公开的操作的计算机程序代码，上述程序设计语言包括但不限于面向对象的程序设计语言——诸如 Java、Smalltalk、C++，

30 还包括常规的过程式程序设计语言——诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网（LAN）或广域网（WAN）——连接到用户计算机，或者，可以连接到外部计算机（例如利用因特网服务提供商来通过因特网连接）。

35

附图中的流程图和框图，图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的

功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

- 5 描述于本公开实施例中所涉及到的模块可以通过软件的方式实现，也可以通过硬件的方式来实现。其中，模块的名称在某种情况下并不构成对该模块本身的限定，例如，第一接收模块还可以被描述为“接收请求消息的模块”。

- 本文中以上描述的功能可以至少部分地由一个或多个硬件逻辑部件来执行。例如，非限制性地，可以使用的示范类型的硬件逻辑部件包括：现场可编程门阵列（Field-Programmable Gate Array, FPGA）、专用集成电路（Application Specific Integrated Circuit, ASIC）、专用标准产品（Application Specific Standard Product, ASSP）、片上系统（System-on-a-chip, SOC）、复杂可编程逻辑设备（Complex Programmable Logic Device, CPLD）等等。

- 在本公开的上下文中，机器可读介质可以是有形的介质，其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的程序。机器可读介质可以是机器可读信号介质或机器可读储存介质。机器可读介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备，或者上述内容的任何合适组合。机器可读储存介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦除可编程只读存储器（EPROM或快闪存储器）、光纤、便捷式紧凑盘只读存储器（CD-ROM）、光学储存设备、磁储存设备、或上述内容的任何合适组合。

- 根据本公开的一个或多个实施例，示例 1 提供了一种传输消息的方法，应用于预设服务器所述预设服务器，为预先部署的在终端和云服务器之间传输消息的服务器，所述方法包括：接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；根据所述云服务访问请求消息确定待访问的云服务接口地址；根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。

- 根据本公开的一个或多个实施例，示例 2 提供了示例 1 的方法，所述根据所述域名地址信息确定待访问的云服务接口地址包括：获取所述预设服务器对应的预设域名后缀；从所述云服务访问请求消息中获取所述域名地址信息；根据所述预设域名后缀从所述域名地址信息中确定所述云服务接口地址。

- 根据本公开的一个或多个实施例，示例 3 提供了示例 1 的方法，所述云服务访问请求消息包括当前用户的用户标识信息和业务请求数据，所述业务请求数据包括所述当前用户待访问的云服务器的对应的云厂商的厂商标识信息，所述根据所述云服务接口地址对所述云服务访问请求消息进行签名验证包括：根据所述云服务接口地址确定所述云服务器对应的签名算法；根据所述用户标识信息和所述厂商标识信息获取当前用户对应的第一密钥，所述第一密钥为所述预设服务器预先生成的；根据所述第一密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第一签名；根据所述第一签名对所述云服务访问请求消息进行签名验证。

根据本公开的一个或多个实施例，示例 4 提供了示例 3 的方法，所述对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息包括：根据所述用户标识信息和所述厂商标识信息获取所述云服务器对应的第二密钥，所述第二密钥为所述云服务器预先生成的；根据所述第二密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第二签名；根据所述第二签名对所述云服务访问请求消息进行重新签名，得到所述新的云服务访问请求消息。

根据本公开的一个或多个实施例，示例 5 提供了示例 1-4 任一项的方法，所述方法还包括：接收所述云服务器根据所述新的云服务访问请求消息发送的云服务访问响应消息，并将所述云服务访问响应消息发送至所述终端。

根据本公开的一个或多个实施例，示例 6 提供了示例 5 的方法，在所述接收所述云服务器根据所述新的云服务访问请求消息发送的云服务访问响应消息后，所述方法还包括：根据所述新的云服务访问请求消息和所述云服务访问响应消息生成访问日志，所述访问日志用于记录当前用户的云服务访问事项。

根据本公开的一个或多个实施例，示例 7 提供了一种传输消息的方法，应用于终端，所述方法包括：获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；将所述云服务访问请求消息发送至所述预设服务器，以便所述预设服务器在对所述云服务访问请求消息进行签名验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

根据本公开的一个或多个实施例，示例 8 提供了示例 7 的方法，所述业务请求数据包括所述当前用户待访问的所述云服务器的对应的云厂商的厂商标识信息，所述根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息包括：根据所述厂商标识信息获取所述云服务器的云服务接口地址；根据所述云服务接口地址和所述预设服务器对应的预设域名后缀生成所述域名地址信息；根据所述访问密钥、所述用户标识信息以及所述业务请求数据采用所述云服务器提供的签名算法生成第三签名；根据所述第三签名、所述用户标识信息、所述业务请求数据以及所述域名地址信息生成所述云服务访问请求消息。

根据本公开的一个或多个实施例，示例 9 提供了一种传输消息的装置，应用于预设服务器，所述预设服务器为预先部署的在终端和云服务器之间传输消息的服务器，所述装置包括：第一接收模块，用于接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；确定模块，用于根据所述云服务访问请求消息确定待访问的云服务接口地址；验证模块，用于根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；第一发送模块，用于根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。

根据本公开的一个或多个实施例，示例 10 提供了示例 9 的装置，所述确定模块，用于获取所述预设服务器对应的预设域名后缀；从所述云服务访问请求消息中获取所述域名地址信息；根据所述预设域名后缀从所述域名地址信息中确定所述云服务接口地址。

根据本公开的一个或多个实施例，示例 11 提供了示例 9 的装置，所述云服务访问请求消息包括当前用户的用户标识信息和业务请求数据，所述业务请求数据包括所述当前用户待访问的云服务器的对应的云厂商的厂商标识信息；所述验证模块，用于根据所述云服务接口地址确定所述云服务器对应的签名算法；根据所述用户标识信息和所述厂商标识信息获取当前用户对应的第一密钥，所述第一密钥为所述预设服务器预先生成的；根据所述第一密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第一签名；根据所述第一签名对所述云服务访问请求消息进行签名验证。

根据本公开的一个或多个实施例，示例 12 提供了示例 11 的装置，所述验证模块，用于根据所述用户标识信息和所述厂商标识信息获取所述云服务器对应的第二密钥，所述第二密钥为所述云服务器预先生成的；根据所述第二密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第二签名；根据所述第二签名对所述云服务访问请求消息进行重新签名，得到所述新的云服务访问请求消息。

根据本公开的一个或多个实施例，示例 13 提供了示例 9-12 任一的装置，所述装置还包括：

第二接收模块，用于接收所述云服务器根据所述新的云服务访问请求消息发送的云服务访问响应消息，并将所述云服务访问响应消息发送至所述终端。

根据本公开的一个或多个实施例，示例 14 提供了示例 13 的装置，所述装置还包括：日志生成模块，用于根据所述新的云服务访问请求消息和所述云服务访问响应消息生成访问日志，所述访问日志用于记录当前用户的云服务访问事项。

根据本公开的一个或多个实施例，示例 15 提供了一种传输消息的装置，应用于终端，所述装置包括：

获取模块，用于获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；

请求消息生成模块，用于根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

第二发送模块，用于将所述云服务访问请求消息发送至所述预设服务器，以便所述预设服务器在对所述云服务访问请求消息进行签名验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

根据本公开的一个或多个实施例，示例 16 提供了示例 15 的装置，所述业务请求数据包括所述当前用户待访问的所述云服务器的对应的云厂商的厂商标识信息，所述请求消息生成模块，用于根据所述厂商标识信息获取所述云服务器的云服务接口地址；根据所述云服务接口地址和所述预设服务器对应的预设域名后缀生成域名地址信息；根据所述访问密钥、所述用户标识信息以及所述业务请求数据采用所述云服务器提供的签名算法生成第三签名；根据所述第三签名、所述用户标识信息、所述业务请求数据以及所述域名地址信息生成所述云服务访问请求消息。

以上描述仅为本公开的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本公开中所涉及的公开范围，并不限于上述技术特征的特定组合而成的技术方案，同

时也应涵盖在不脱离上述公开构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本公开中公开的（但不限于）具有类似功能的技术特征进行互相替换而形成的技术方案。

5 此外，虽然采用特定次序描绘了各操作，但是这不应理解为要求这些操作以所示出的特定次序或以顺序次序执行来执行。在一定环境下，多任务和并行处理可能是有利的。同样地，虽然在上面论述中包含了若干具体实现细节，但是这些不应被解释为对本公开的范围的限制。在单独的实施例的上下文中描述的某些特征还可以组合地实现在单个实施例中。相反地，在单个实施例的上下文中描述的各种特征也可以单独地或以任何合适的子组合的方式实现在多个实施例中。

10 尽管已经采用特定于结构特征和/或方法逻辑动作的语言描述了本主题，但是应当理解所附权利要求书中所限定的主题未必局限于上面描述的特定特征或动作。相反，上面所描述的特定特征和动作仅仅是实现权利要求书的示例形式。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。

15

权 利 要 求 书

- 1、一种传输消息的方法，应用于预设服务器，所述预设服务器为预先部署的在终端和云服务器之间传输消息的服务器，所述方法包括：
- 接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；
- 5 根据所述云服务访问请求消息确定待访问的云服务接口地址；
- 根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；
- 根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。
- 10 2、根据权利要求1所述的方法，其中，所述根据所述云服务访问请求消息确定待访问的云服务接口地址包括：
- 获取所述预设服务器对应的预设域名后缀；
- 从所述云服务访问请求消息中获取所述域名地址信息；
- 根据所述预设域名后缀从所述域名地址信息中确定所述云服务接口地址。
- 15 3、根据权利要求1或2所述的方法，其中，所述云服务访问请求消息包括当前用户的用户标识信息和业务请求数据，所述业务请求数据包括所述当前用户待访问的所述云服务器的对应的云厂商的厂商标识信息，所述根据所述云服务接口地址对所述云服务访问请求消息进行签名验证包括：
- 根据所述云服务接口地址确定所述云服务器对应的签名算法；
- 20 根据所述用户标识信息和所述厂商标识信息获取当前用户对应的第一密钥，所述第一密钥为所述预设服务器预先生成的；
- 根据所述第一密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第一签名；
- 根据所述第一签名对所述云服务访问请求消息进行签名验证。
- 25 4、根据权利要求3所述的方法，其中，所述对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息包括：
- 根据所述用户标识信息和所述厂商标识信息获取所述云服务器对应的第二密钥，所述第二密钥为所述云服务器预先生成的；
- 根据所述第二密钥、所述用户标识信息以及所述业务请求数据采用所述签名算法生成第二签名；
- 30 根据所述第二签名对所述云服务访问请求消息进行重新签名，得到所述新的云服务访问请求消息。
- 5、根据权利要求1-4任一项所述的方法，其中，所述方法还包括：
- 接收所述云服务器根据所述新的云服务访问请求消息发送的云服务访问响应消息，并将
- 35 所述云服务访问响应消息发送至所述终端。
- 6、根据权利要求5所述的方法，其中，在所述接收所述云服务器根据所述新的云服务访问请求消息发送的云服务访问响应消息后，所述方法还包括：
- 根据所述新的云服务访问请求消息和所述云服务访问响应消息生成访问日志，所述访问日志用于记录当前用户的云服务访问事项。

7、一种传输消息的方法，应用于终端，所述方法包括：

获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；

根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息，  
5 所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

将所述云服务访问请求消息发送至所述预设服务器，以便所述预设服务器在对所述云服务访问请求消息进行签名验证并验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

8、根据权利要求7所述的方法，其中，所述业务请求数据包括所述当前用户待访问的所述  
10 所述服务器的对应的云厂商的厂商标识信息，所述根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息包括：

根据所述厂商标识信息获取所述云服务器的云服务接口地址；

根据所述云服务接口地址和所述预设服务器对应的预设域名后缀生成所述域名地址信息；

15 根据所述访问密钥、所述用户标识信息以及所述业务请求数据采用所述云服务器提供的签名算法生成第三签名；

根据所述第三签名、所述用户标识信息、所述业务请求数据以及所述域名地址信息生成所述云服务访问请求消息。

9、一种传输消息的装置，应用于预设服务器，所述预设服务器为预先部署的在终端和云  
20 服务器之间传输消息的服务器，所述装置包括：

第一接收模块，用于接收所述终端发送的云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

确定模块，用于根据所述云服务访问请求消息确定待访问的云服务接口地址；

25 验证模块，用于根据所述云服务接口地址对所述云服务访问请求消息进行签名验证，并在验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息；

第一发送模块，用于根据所述云服务接口地址将所述新的云服务访问请求消息发送至所述云服务器。

10、一种传输消息的装置，应用于终端，所述装置包括：

30 获取模块，用于获取当前用户的用户标识信息、业务请求数据以及预设服务器为所述当前用户预先分配的访问密钥，所述预设服务器为预先部署的在所述终端和云服务器之间传输消息的服务器；

请求消息生成模块，用于根据所述用户标识信息、所述业务请求数据以及所述访问密钥生成云服务访问请求消息，所述云服务访问请求消息中包括所述预设服务器的域名地址信息；

35 第二发送模块，用于将所述云服务访问请求消息发送至所述预设服务器，以便所述预设服务器在对所述云服务访问请求消息进行签名验证并验证通过的情况下，对所述云服务访问请求消息进行重新签名，得到新的云服务访问请求消息，并将所述新的云服务访问请求消息发送至所述云服务器。

11、一种计算机可读存储介质，其上存储有计算机程序，其中，所述计算机程序被处理

装置执行时实现权利要求 1-6 或权利要求 7-8 中任一项所述方法的步骤。

12、一种电子设备，包括：

存储装置，其上存储有至少一个计算机程序；

至少一个处理装置，用于执行所述存储装置中的所述至少一个计算机程序，以实现权利

5 要求 1-6 或权利要求 7-8 中任一项所述方法的步骤。

13、一种计算机程序产品，包括计算机指令，其中，所述计算机指令被处理装置执行时实现权利要求 1-6 或权利要求 7-8 中任一项所述方法的步骤。

14、一种计算机程序，其中，所述计算机程序被处理装置执行时实现权利要求 1-6 或权利要求 7-8 中任一项所述方法的步骤。

10