(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105376242 A
(43)申请公布日 2016.03.02

(21)申请号 201510847030.0

(22)申请日 2015.11.26

(71)申请人 上海斐讯数据通信技术有限公司
地址 201616 上海市松江区思贤路3666号

(72)发明人 余启轩

(74)专利代理机构 上海光华专利事务所 31219
代理人 王再朝

(51)Int.Cl.
H04L 29/06(2006.01)

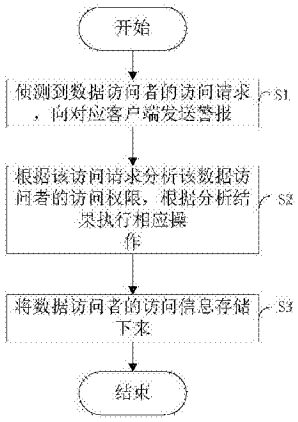
权利要求书2页 说明书9页 附图3页

(54)发明名称

一种云终端数据访问的认证方法、系统及云终端的管理系统

(57)摘要

本发明提供一种云终端数据访问的认证方法、系统及云终端的管理系统，所述认证方法包括以下步骤：S1、侦测到数据访问者的访问请求，向对应客户端发送警报；S2、根据所述访问请求分析所述数据访问者的访问权限，根据分析结果执行相应操作，当所述访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权所述数据访问者进行访问。本发明中，当侦测到有数据请求时，分析该数据请求是否携带密钥，以便对数据访问者进行身份核实，当该数据请求携带密匙时，该数据访问者为正常访问者，对其进行授权访问，当该访问请求不携带密钥时，其数据访问者为非法访问，拒绝其访问请求，由于使用密钥对来进行数据加密及解密，可保证数据的安全性。



CN 105376242 A

1. 一种云终端数据访问的认证方法，其特征在于，所述认证方法包括以下步骤：

S1、侦测到数据访问者的访问请求，向对应客户端发送警报；

S2、根据所述访问请求分析所述数据访问者的访问权限，根据分析结果执行相应操作，当所述访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权所述数据访问者进行访问。

2. 根据权利要求 1 所述的认证方法，其特征在于：所述步骤 S1 具体包括：

S11、将客户端用户的身份信息转化为数字代码，形成所述密钥对，所述密钥对包括公钥及对应的私钥；

S12、基于所述密钥对对所述客户端的数据进行加密处理，获得加密数据；

S13、侦测到数据访问者的访问请求，基于该访问请求向对应客户端发送警报。

3. 根据权利要求 2 所述的认证方法，其特征在于：所述步骤 S12 具体为：根据所述公钥对所述数据进行加密，获得加密数据；

所述步骤 S2 具体包括：

S21、分析所述访问请求，判断所述访问请求是否携带所述私钥，当判断结果为是，确认为正常访问，转到步骤 S22，否则确认为非法访问，转到步骤 S23；

S22、对所述数据访问者进行授权，允许所述数据访问者进行数据访问；

S23、拒绝该数据访问者的访问请求。

4. 根据权利要求 1 所述的认证方法，其特征在于：所述步骤 S12 具体为：根据所述私钥对所述数据进行加密，获得加密数据；

所述步骤 S2 具体包括：

S81、分析所述访问请求，判断所述访问请求是否携带所述公钥，当判断结果为是，确认为正常访问，转到步骤 S82，否则确认为非法访问，转到步骤 S83；

S82、对所述数据访问者进行授权，允许所述数据访问者进行数据访问；

S83、拒绝所述数据访问者的访问请求。

5. 根据权利要求 3 或 4 所述的认证方法，其特征在于：所述禁止对所述数据访问者的访问请求步骤之后，还包括：

将所述数据访问者的访问信息存储下来。

6. 一种云终端数据访问的认证系统，其特征在于：所述认证系统包括：

侦测模块，用于实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报；

与所述侦测模块连接的访问控制模块，用于根据所述访问请求分析所述数据访问者的访问权限，根据分析结果执行相应操作，当所述访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权所述数据访问者进行访问。

7. 根据权利要求 6 所述的认证系统，其特征在于，所述侦测模块具体包括：

转化单元，用于将客户端用户的身份信息转化为数字代码，形成所述密钥对，所述密钥对包括公钥及对应的私钥；

与所述转化单元连接的加密单元，用于基于所述密钥对对所述客户端的数据进行加密处理，获得加密数据；

与所述加密单元连接的侦测单元，用于实时侦测是否有数据访问者对云终端的服务器

的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报。

8. 根据权利要求 7 所述的认证系统，其特征在于，所述加密单元具体用于基于所述公钥对所述客户端的数据进行加密处理，获得加密数据；

所述访问控制模块具体包括：

第一判断单元，用于分析所述访问请求，判断所述访问请求是否携带所述私钥，当判断结果为是确认为正常访问，否则确认为非法访问；

与所述第一判断单元连接的第一授权单元，用于当确认为正常访问时，对所述数据访问者进行授权，允许所述数据访问者进行数据访问；

与所述第一判断单元连接的第一拒绝单元，用于当确认为非法访问时，拒绝该数据访问者的访问请求。

9. 根据权利要求 7 所述的认证系统，其特征在于，所述加密单元具体用于基于所述私钥对所述客户端的数据进行加密处理，获得加密数据；

所述访问控制模块具体包括：

第二判断单元，用于分析所述访问请求，判断所述访问请求是否携带所述公钥，当判断结果为是，确认为正常访问，否则确认为非法访问；

与所述第二判断单元连接的第二授权单元，用于当确认为正常访问时，对所述数据访问者进行授权，允许所述数据访问者进行数据访问；

与所述第二判断单元连接的第二拒绝单元，用于当确认为非法访问时，拒绝该数据访问者的访问请求。

10. 一种云终端的管理系统，其特征在于，包括如权利要求 6 至 9 任意一项所述的认证系统。

一种云终端数据访问的认证方法、系统及云终端的管理系统

技术领域

[0001] 本发明涉及一种网络技术领域，特别是涉及一种云终端数据访问的认证方法、系统及云终端的管理系统。

背景技术

[0002] 云计算是当前信息技术领域的热门话题之一，是产业界、学术界、政府等各界均十分关注的焦点。它体现了“网络就是计算机”的思想，将大量计算资源、存储资源与软件资源链接在一起，形成巨大规模的共享虚拟 IT 资源池。

[0003] 但是，使用云计算服务，用户并不是清楚自己的数据具体的托管服务器所在的位置以及具体由哪个服务器管理。例如数据在云服务中的存储是共享的，即没有为用户开辟独立存储区。因此数据具有潜在危险；又例如，目前在网络中用户基本采用数据加密方式共享数据，但未能将自己的数据与其他用户的数据隔离开，因而数据的隐私即数据的安全隔离存在一定的隐患，云的特殊存储结构使得隐私保持成为一个关键的安全问题。

[0004] 目前应用最多的方法就是对上传到云终端的数据进行混淆和加密，但密码会由于过于简单或者符合某种规律而被识别出来，服务器容易被非法用户访问而导致数据的不安全。

发明内容

[0005] 鉴于以上所述现有技术的缺点，本发明的目的在于提供一种云终端数据访问的认证方法、系统及云终端的管理系统，用于解决现有技术中存储在云终端的数据容易被访问而导致不安全的问题。

[0006] 为实现上述目的及其他相关目的，本发明提供一种云终端数据访问的认证方法、系统及云终端的管理系统；其中，所述云终端数据访问的认证方法包括以下步骤：S1、侦测到数据访问者的访问请求，向对应客户端发送警报；S2、根据所述访问请求分析所述数据访问者的访问权限，根据分析结果执行相应操作，当所述访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权所述数据访问者进行访问。

[0007] 于本发明的一实施方式中，所述步骤 S1 具体包括：S11、将客户端用户的身份信息转化为数字代码，形成所述密钥对，所述密钥对包括公钥及对应的私钥；S12、基于所述密钥对对所述客户端的数据进行加密处理，获得加密数据；S13、侦测到数据访问者的访问请求，基于该访问请求向对应客户端发送警报。

[0008] 于本发明的一实施方式中，所述步骤 S12 具体为：根据所述公钥对所述数据进行加密，获得加密数据；所述步骤 S2 具体包括：S21、分析所述访问请求，判断所述访问请求是否携带所述私钥，当判断结果为是，确认为正常访问，转到步骤 S22，否则确认为非法访问，转到步骤 S23；S22、对所述数据访问者进行授权，允许所述数据访问者进行数据访问；S23、拒绝该数据访问者的访问请求。

[0009] 于本发明的一实施方式中，所述步骤 S12 具体为：根据所述私钥对所述数据进行加密，获得加密数据；所述步骤 S2 具体包括：S81、分析所述访问请求，判断所述访问请求是否携带所述公钥，当判断结果为是，确认为正常访问，转到步骤 S82，否则确认为非法访问，转到步骤 S83；S82、对所述数据访问者进行授权，允许所述数据访问者进行数据访问；S83、拒绝所述数据访问者的访问请求。

[0010] 于本发明的一实施方式中，所述禁止对所述数据访问者的访问请求步骤之后，还包括：将所述数据访问者的访问信息存储下来。

[0011] 本发明还提供一种云终端数据访问的认证系统，所述认证系统包括：侦测模块，用于实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报；与所述侦测模块连接的访问控制模块，用于根据所述访问请求分析所述数据访问者的访问权限，根据分析结果执行相应操作，当所述访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权所述数据访问者进行访问。

[0012] 于本发明的一实施方式中，所述侦测模块具体包括：转化单元，用于将客户端用户的身份信息转化为数字代码，形成所述密钥对，所述密钥对包括公钥及对应的私钥；与所述转化单元连接的加密单元，用于基于所述密钥对对所述客户端的数据进行加密处理，获得加密数据；与所述加密单元连接的侦测单元，用于实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报。

[0013] 于本发明的一实施方式中，所述加密单元具体用于基于所述公钥对所述客户端的数据进行加密处理，获得加密数据；所述访问控制模块具体包括：第一判断单元，用于分析所述访问请求，判断所述访问请求是否携带所述私钥，当判断结果为是确认为正常访问，否则确认为非法访问；与所述第一判断单元连接的第一授权单元，用于当确认为正常访问时，对所述数据访问者进行授权，允许所述数据访问者进行数据访问；与所述第一判断单元连接的第一拒绝单元，用于当确认为非法访问时，拒绝该数据访问者的访问请求。

[0014] 于本发明的一实施方式中，所述加密单元具体用于基于所述私钥对所述客户端的数据进行加密处理，获得加密数据；

[0015] 所述访问控制模块具体包括：第二判断单元，用于分析所述访问请求，判断所述访问请求是否携带所述公钥，当判断结果为是，确认为正常访问，否则确认为非法访问；与所述第二判断单元连接的第二授权单元，用于当确认为正常访问时，对所述数据访问者进行授权，允许所述数据访问者进行数据访问；与所述第二判断单元连接的第二拒绝单元，用于当确认为非法访问时，拒绝该数据访问者的访问请求。

[0016] 本发明还提供一种云终端的管理系统，所述管理系统包括云终端数据访问的认证系统，所述认证系统包括：侦测模块，用于实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报；与所述侦测模块连接的访问控制模块，用于根据所述访问请求分析所述数据访问者的访问权限，根据分析结果执行相应操作，当所述访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权所述数据访问者进行访问。

[0017] 本发明的一种云终端数据访问的认证方法、系统及云终端的管理系统，至少具有以下有益效果：

[0018] 当侦测到有数据请求时，分析该数据请求是否携带密钥，以便对数据访问者进行

身份核实，当该数据请求携带时密匙，该数据访问者为正常访问者，对其进行授权访问，当该访问请求不携带密钥时，其数据访问者为非法访问，拒绝其访问请求，由于使用密钥对来进行数据加密及解密，可保证数据的安全性。

附图说明

[0019] 图 1 是本发明的一种云终端数据访问的认证方法一实施例的流程示意图；

[0020] 图 2 是本发明的一种云终端数据访问的认证方法的步骤 S1 的具体流程图；

[0021] 图 3 是本发明的一种云终端数据访问的认证方法的一优选实施例的步骤 S2 的具体流程图；

[0022] 图 4 是本发明的一种云终端数据访问的认证方法的另一优选实施例的步骤 S2 的具体流程图；

[0023] 图 5 是本发明提供一种云终端数据访问的认证系统一实施例的结构示意图；

[0024] 图 6 是本发明的一种云终端数据访问的认证系统的侦测模块 1 的具体结构图；

[0025] 图 7 是本发明的一种云终端数据访问的认证系统的一优选实施例的访问控制模块 2 的具体结构图；

[0026] 图 8 是本发明的一种云终端数据访问的认证系统的另一优选实施例的访问控制模块 2 的具体结构图。

[0027] 元件标号说明：

[0028] 1 侦测模块

[0029] 2 访问控制模块

[0030] 3 存储模块

[0031] 11 转化单元

[0032] 12 加密单元

[0033] 13 侦测单元

[0034] 21 第一判断单元

[0035] 22 第一授权单元

[0036] 23 第一拒绝单元

[0037] 81 第二判断单元

[0038] 82 第二授权单元

[0039] 83 第二拒绝单元

[0040] S1 ～ S43 步骤

具体实施方式

[0041] 以下通过特定的具体实例说明本发明的实施方式，本领域技术人员可由本说明书所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用，本说明书中的各项细节也可以基于不同观点与应用，在没有背离本发明的精神下进行各种修饰或改变。需说明的是，在不冲突的情况下，以下实施例及实施例中的特征可以相互组合。

[0042] 需要说明的是，以下实施例中所提供的图示仅以示意方式说明本发明的基本构

想，遂图式中仅显示与本发明中有关的组件而非按照实际实施时的组件数目、形状及尺寸绘制，其实际实施时各组件的型态、数量及比例可为一种随意的改变，且其组件布局型态也可能更为复杂。

[0043] 实施例 1

[0044] 请参阅图 1，为本发明的一种云终端数据访问的认证方法一实施例的流程示意图，所述认证方法包括步骤：

[0045] 步骤 S1、侦测到数据访问者的访问请求，向对应客户端发送警报；

[0046] 其中，实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报；具体地，云终端包括有若干服务器（具体为大量服务器），每个服务器有与其连接的对应客户端，该服务器存储客户端的数据，当有数据访问者访问该服务器时，会发送访问请求，基于该访问请求找到对应的客户端，然后向客户端发送警报，以告知该客户端有数据访问者访问其存储的数据，使其第一时间识别该数据访问者的访问权限，及时保护数据的安全。进一步地，该警报可包括用户自身正常访问或非用户自身正常访问，此时为了及时向对应客户端发送警报，不对访问请求进行分析识别，因此仅识别是否为对应客户端用户自身访问进行识别。

[0047] 步骤 S2、根据该访问请求分析该数据访问者的访问权限，根据分析结果执行相应操作，当该访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权数据访问者进行访问。

[0048] 其中，需要对访问请求进行分析，具体可分析访问请求是否携带密钥对中的公钥或私钥，该密钥对是一种数字身份证，可通过将客户端的真实身份信息转化为数字代码，可通过网络等相关设备进行识别和查询的公共密钥对，其包括公钥（也可以成为密钥）及私钥（也可以成为密钥），公钥是密钥对中公开的部分，而私钥是不公开的部分，公钥通常用于加密会话密钥、验证数字签名、或加密数据等，但该加密数据必须用对应私钥进行解密。而私钥是由公开可信的专用密钥生成器 PKG(Private Key Generator) 结合用户身份来生成，该私钥或公钥均可用来结合客户端的真实身份信息来加密数据，但二者是成对出现的，当其中一个用于加密数据时，用另外一个才能解密该加密数据。这样就保证了数据的绝对安全性。进一步地，当用其中一个进行数据加密时，该加密数据存储在云终端的服务器中，而另一个则发送给对应的客户端，该客户端会根据实际请求向需要访问该数据的合法访问者（例如其他客户端用户）发送该密钥对，便于该合法访问者需要访问数据时，发送携带该密钥对中的一个来进行身份认证，核实身份后，进行数据解密。

[0049] 本实施例中，实时监测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者，基于访问请求是否携带密钥对中的私钥或公钥，可核实数据访问者的合法性，当核实为正常访问时，对该数据访问者进行授权，由于使用密钥对进行数据认证，可一定程度上保证数据访问的安全性。

[0050] 进一步于本发明的一实施方式中，所述认证方法还包括以下步骤：

[0051] 步骤 S3、将数据访问者的访问信息存储下来。

[0052] 其中，该访问信息可包括访问者身份、网络地址、访问请求及访问原因等，此处对此不做限制。具体地，可对该访问信息进行分类存储，具体可分为授权 / 非授权、或正常 / 异常、或恶意 / 非恶意、或服务器提供方 / 非服务器提供方、或常见访问 \ 非常见访问、或部

分内容解密访问 / 全部明文解密访问、或安全级别较高访问者 / 安全级别较低访问者。进一步地，所述认证方法还可包括步骤：将访问信息反馈给对应客户端，以供客户端用户根据访问信息进行一些操作，例如根据实际情况对部分非授权或非恶意数据访问者进行部分授权，使其可对一些数据进行访问。对一些恶意访问者进行限制或禁止访问；或对部分安全级别较高访问者进行授权访问或对其开放优先访问权限等；对部分安全级别较低访问者进行限制访问或给予低优先级访问权限。

[0053] 如图 2 所示，为本发明的一种云终端数据访问的认证方法的步骤 S1 的具体流程图，所述步骤 S1 具体包括：

[0054] 步骤 S11、将客户端用户的身份信息转化为数字代码，形成密钥对，该密钥对包括公钥及对应的私钥；；

[0055] 将客户端用户的真实身份信息通过转化算法转化为数字代码，形成密钥对，具体可采用现有的转化算法，此处不赘述。此密钥对可为对称或非对称密钥对，于本发明的一实施方式中，此处密钥对为非对称密钥对。

[0056] 步骤 S12、基于密钥对对客户端的数据进行加密处理，获得加密数据；

[0057] 对客户端存储在服务器的数据进行加密处理，使用上述密钥对来进行加密，可使用私钥或公钥来对该数据进行加密处理。可采用现有技术对上述数据进行加密，此处不再赘述。

[0058] 步骤 S13、侦测到数据访问者的访问请求，基于该访问请求向对应客户端发送警报。

[0059] 具体地，实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报。此时不对访问请求进行任何处理，而及时向对应客户端反馈有数据访问者的警报，可提醒用户，一定程度上保证数据的安全性。

[0060] 在本实施例的一个优选方案中，所述步骤 S12 中，具体为根据该公钥对数据进行加密处理，获得加密数据。如图 3 所示，为本发明的一种云终端数据访问的认证方法的一优选实施例的步骤 S2 的具体流程图，所述步骤 S2 的具体过程如下：

[0061] 步骤 S21、分析访问请求，判断所述访问请求是否携带所述私钥，当判断结果为是，确认为正常访问，转到步骤 S22，否则确认为非法访问，转到步骤 S23；

[0062] 具体地，分析该访问请求，如果该访问请求携带私钥，则说明是合法用户的正常访问，如果不携带则说明该数据访问者是非正常访问，由于在前述步骤中是使用公钥对数据进行加密，此时必须使用私钥对数据进行解密，此时该访问请求需要携带该私钥才能进行访问。由于该密钥对为非对称密钥对，相比于普通的密码加密，此处使用非对称密钥对进行数据加密及解密，。可大大提高数据的安全性。

[0063] 步骤 S22、对数据访问者进行授权，允许数据访问者进行数据访问；

[0064] 当该访问请求携带私钥时，说明该访问者为合法访问者，即已经得到对应客户端的授权。此时对该数据访问者进行授权，允许其进行数据访问。

[0065] S23、拒绝该数据访问者的访问请求。

[0066] 当访问请求不携带该私钥时，说明访问者不是合法访问者，即没有得到对应客户端的授权，此时拒绝对该数据访问者的访问请求，使其无权进行数据访问。

[0067] 在另外一个优选方案中，所述步骤 S12 中，具体为根据该私钥对数据进行加密处

理，获得加密数据。如图 4 所示，为本发明的一种云终端数据访问的认证方法的另一优选实施例的步骤 S2 的具体流程图，所述步骤 S2 的具体过程如下：

[0068] 步骤 S41、分析访问请求，判断所述访问请求是否携带所述公钥，当判断结果为是，确认为正常访问，转到步骤 S42，否则确认为非法访问，转到步骤 S43；

[0069] 具体地，分析该访问请求，如果该访问请求携带公钥，则说明是合法用户的正常访问，如果不携带则说明该数据访问者是非正常访问，由于在前述步骤中是使用私钥对数据进行加密，此时必须使用公钥对数据进行解密，此时该访问请求需要携带该公钥才能进行访问。由于该密钥对为非对称密钥对，相比于普通的密码加密，此处使用非对称密钥对进行数据加密及解密，可大大提高数据的安全性。

[0070] 步骤 S42、对数据访问者进行授权，允许数据访问者进行数据访问；

[0071] 当该访问请求携带公钥时，说明该访问者为合法访问者，即已经得到对应客户端的授权。此时对该数据访问者进行授权，允许其进行数据访问。

[0072] S43、拒绝该数据访问者的访问请求。

[0073] 当访问请求不携带该公钥时，说明访问者不是合法访问者，即没有得到对应客户端的授权，此时拒绝对该数据访问者的访问请求，使其无权进行数据访问。

[0074] 本实施例中，侦测到有访问请求时，基于访问请求及与数据对应的密钥对识别数据访问者的合法性，当为合法时给其授权，当为非法时拒绝其请求，由于使用非对称性密钥对，可有效保证数据的安全性。

[0075] 此外，在接收到访问请求时，立即给对应客户端发送警报，便于客户端用户及时判断数据访问者的合法性，进一步保证数据的安全性。

[0076] 实施例 2

[0077] 请参阅图 5，为本发明提供一种云终端数据访问的认证系统一实施例的结构示意图，其中所述系统包括终端，所述终端具体包括：侦测模块 1 及与其连接的访问控制模块 2，其中，

[0078] 侦测模块 1，用于实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报；

[0079] 侦测模块 1 实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报；具体地，云终端包括有若干服务器（具体为大量服务器），每个服务器有与其连接的对应客户端，该服务器存储客户端的数据，当有数据访问者访问该服务器时，会发送访问请求，基于该访问请求找到对应的客户端，然后向客户端发送警报，以告知该客户端有数据访问者访问其存储的数据，使其第一时间识别该数据访问者的访问权限，及时保护数据的安全。进一步地，该警报可包括用户自身正常访问或非用户自身正常访问，此时为了及时向对应客户端发送警报，不对访问请求进行分析识别，因此仅识别是否为对应客户端用户自身访问进行识别。

[0080] 访问控制模块 2，用于根据所述访问请求分析所述数据访问者的访问方式，根据分析结果执行相应操作，当所述访问请求携带密钥对中的私钥或公钥时，确认该访问方式为正常访问，授权所述数据访问者进行访问。

[0081] 其中，需要对访问请求进行分析，具体可分析访问请求是否携带密钥对中的公钥或私钥，该密钥对是一种数字身份证，可通过将客户端的真实身份信息转化为数字代码，可

通过网络等相关设备进行识别和查询的公共密钥对，其包括公钥及私钥，公钥是密钥对中公开的部分，而私钥是不公开的部分，公钥通常用于加密会话密钥、验证数字签名、或加密数据等，但该加密数据必须用对应私钥进行解密。而私钥是由公开可信的专用密钥生成器PKG(Private Key Generator)结合用户身份来生成，该私钥或公钥均可用来结合客户端的真实身份信息来加密数据，但二者是成对出现的，当其中一个用于加密数据时，用另外一个才能解密该加密数据。这样就保证了数据的绝对安全性。进一步地，当用其中一个进行数据加密时，该加密数据存储在云终端的服务器中，而另一个则发送给对应的客户端，该客户端会根据实际请求向需要访问该数据的合法访问者（例如其他客户端用户）发送该密钥对，便于该合法访问者需要访问数据时，发送携带该密钥对中的一个来进行身份认证，核实身份后，进行数据解密。

[0082] 本实施例中，实时监测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者，基于访问请求是否携带密钥对中的私钥或公钥，可核实数据访问者的合法性，当核实为正常访问时，对该数据访问者进行授权，由于使用密钥对进行数据认证，可一定程度上保证数据访问的安全性。

[0083] 进一步于本发明的一实施方式中，所述认证系统还包括与所述访问控制模块2连接的存储模块3；

[0084] 存储模块3、用于将数据访问者的访问信息存储下来。

[0085] 其中，该访问信息可包括访问者身份、网络地址、访问请求及访问原因等，此处对此不做限制。具体地，可对该访问信息进行分类存储，具体可分为授权/非授权、或正常/异常、或恶意/非恶意、或服务器提供方/非服务器提供方、或常见访问\非常见访问、或部分内容解密访问/全部明文解密访问、或安全级别较高访问者/安全级别较低访问者。进一步地，所述认证系统还可包括反馈模块，用于将访问信息反馈给对应客户端，以供客户端用户根据访问信息进行一些操作，例如根据实际情况对部分非授权或非恶意数据访问者进行部分授权，使其可对一些数据进行访问。对一些恶意访问者进行限制或禁止访问；或对部分安全级别较高访问者进行授权访问或对其开放优先访问权限等；对部分安全级别较低访问者进行限制访问或给予低优先级访问权限。

[0086] 如图6所示，为本发明的一种云终端数据访问的认证系统的侦测模块1的具体结构图，所述侦测模块1具体包括：转化单元11、与所述转化单元11连接的加密单元12、及与该加密单元12连接的侦测单元13；其中：

[0087] 转化单元11，用于将客户端用户的身份信息转化为数字代码，形成所述密钥对，所述密钥对包括公钥及对应的私钥；

[0088] 具体地，将客户端用户的真实身份信息通过转化算法转化为数字代码，形成密钥对。此密钥对可为对称或非对称密钥对，于本发明的一实施方式中，此处密钥对为非对称密钥对。

[0089] 加密单元12，用于基于所述密钥对对所述客户端的数据进行加密处理，获得加密数据；

[0090] 具体地，对客户端存储在服务器的数据进行加密处理，使用上述密钥对来进行加密，可使用私钥或公钥来对该数据进行加密处理。可采用现有技术对上述数据进行加密，此处不再赘述。

[0091] 侦测单元 13，用于实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报。

[0092] 具体地，实时侦测是否有数据访问者对云终端的服务器的数据访问，当侦测到数据访问者的访问请求时，向对应客户端发送警报。此时不对访问请求进行任何处理，而及时向对应客户端反馈有数据访问者的警报，可提醒用户，一定程度上保证数据的安全性。

[0093] 在本实施例的一个优选方案中，该加密单元 12 具体用于基于公钥对客户端的数据进行加密处理，获得加密数据；如图 7 所示，为本发明的一种云终端数据访问的认证系统的一优选实施例的访问控制模块 2 的具体结构图，该访问控制模块 2 具体包括：第一判断单元 21、与该第一判断单元 21 连接的第一授权单元 22，及与该第一判断单元 21 连接的第一拒绝单元 23。

[0094] 第一判断单元 21，用于分析所述访问请求，判断所述访问请求是否携带所述私钥，当判断结果为是确认为正常访问，否则确认为非法访问；

[0095] 具体地，该第一判断单元 21 分析该访问请求，如果该访问请求携带私钥，则说明是合法用户的正常访问，如果不携带则说明该数据访问者是非正常访问，由于在上述加密单元 12 中是使用公钥对数据进行加密，此时必须使用私钥对数据进行解密，此时该访问请求需要携带该私钥才能进行访问。由于该密钥对为非对称密钥对，相比于普通的密码加密，此处使用非对称密钥对进行数据加密及解密，。可大大提高数据的安全性。

[0096] 第一授权单元 22，用于当确认为正常访问时，对所述数据访问者进行授权，允许所述数据访问者进行数据访问；

[0097] 当该访问请求携带私钥时，说明该访问者为合法访问者，即已经得到对应客户端的授权。此时对该数据访问者进行授权，允许其进行数据访问。

[0098] 第一拒绝单元 23，用于当确认为非法访问时，拒绝该数据访问者的访问请求。

[0099] 当访问请求不携带该私钥时，说明访问者不是合法访问者，即没有得到对应客户端的授权，此时拒绝对该数据访问者的访问请求，使其无权进行数据访问。

[0100] 在本实施例的另一个优选方案中，该加密单元 12 具体用于基于私钥对客户端的数据进行加密处理，获得加密数据；如图 8 所示，为本发明的一种云终端数据访问的认证系统的另一优选实施例的访问控制模块 2 的具体结构图，该访问控制模块 2 具体包括：第二判断单元 81、与该第二判断单元 81 连接的第二授权单元 82，及与该第二判断单元 81 连接的第二拒绝单元 83。

[0101] 第二判断单元 21，用于分析访问请求，判断访问请求是否携带所述公钥，当判断结果为是确认为正常访问，否则确认为非法访问；

[0102] 具体地，该第二判断单元 81 分析该访问请求，如果该访问请求携带公钥，则说明是合法用户的正常访问，如果不携带则说明该数据访问者是非正常访问，由于上述加密单元 12 是使用私钥对数据进行加密，此时必须使用公钥对数据进行解密，此时该访问请求需要携带该公钥才能进行访问。由于该密钥对为非对称密钥对，相比于普通的密码加密，此处使用非对称密钥对进行数据加密及解密，可大大提高数据的安全性。

[0103] 第二授权单元 82，用于当确认为正常访问时，对所述数据访问者进行授权，允许所述数据访问者进行数据访问；

[0104] 当该访问请求携带公钥时，说明该访问者为合法访问者，即已经得到对应客户端

的授权。此时对该数据访问者进行授权，允许其进行数据访问。

[0105] 第二拒绝单元 83，用于当确认为非法访问时，拒绝该数据访问者的访问请求。

[0106] 当访问请求不携带该公钥时，说明访问者不是合法访问者，即没有得到对应客户端的授权，此时拒绝对该数据访问者的访问请求，使其无权进行数据访问。

[0107] 本实施例中，侦测到有访问请求时，基于访问请求及与数据对应的密钥对识别数据访问者的合法性，当为合法时给其授权，当为非法时拒绝其请求，由于使用非对称性密钥对，可有效保证数据的安全性。

[0108] 此外，在接收到访问请求时，立即给对应客户端发送警报，便于客户端用户及时判断数据访问者的合法性，进一步保证数据的安全性。

[0109] 基于上述实施例，本发明还提供一种云终端的管理系统，该云终端包括有大量的服务器，而服务器可存储客户端的数据，其中需要对该数据进行加密处理以保证数据不被随意访问，而保证数据的安全性，该管理系统设置有云终端数据访问的认证系统，用于保证数据访问的安全性，该认证系统的具体结构及工作原理与上述实施例所述的基本一致，具体可参考上述实施例，此处不再赘述。

[0110] 综上所述，本发明的一种云终端数据访问的认证方法、系统及云终端，使用密钥对进行数据加密及解密，当侦测到有数据请求时，分析该数据请求是否携带密钥，以便对数据访问者进行身份核实，当该数据请求携带时密钥（即私钥或公钥），该数据访问者为正常访问者，对其进行授权访问，当该访问请求不携带密钥时，其数据访问者为非法访问，拒绝其访问请求，由于使用密钥对来进行数据加密及解密，可保证数据的安全性。所以，本发明有效克服了现有技术中的种种缺点而具高度产业利用价值。

[0111] 上述实施例仅例示性说明本发明的原理及其功效，而非用于限制本发明。任何熟悉此技术的人士皆可在不违背本发明的精神及范畴下，对上述实施例进行修饰或改变。因此，举凡所属技术领域中具有通常知识者在未脱离本发明所揭示的精神与技术思想下所完成的一切等效修饰或改变，仍应由本发明的权利要求所涵盖。

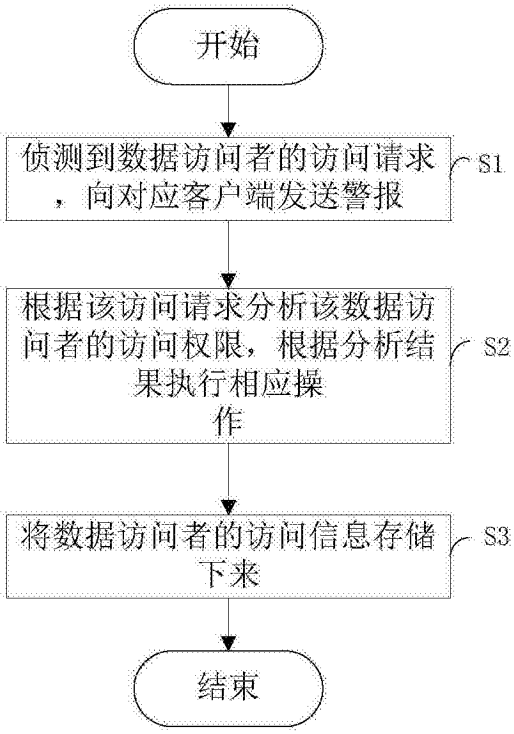

开始
侦测到数据访问者的访问请求，向对应客户端发送警报
S1
根据该访问请求分析该数据访问者的访问权限，根据分析结果执行相应操作
S2
将数据访问者的访问信息存储下来
S3
结束

图 1

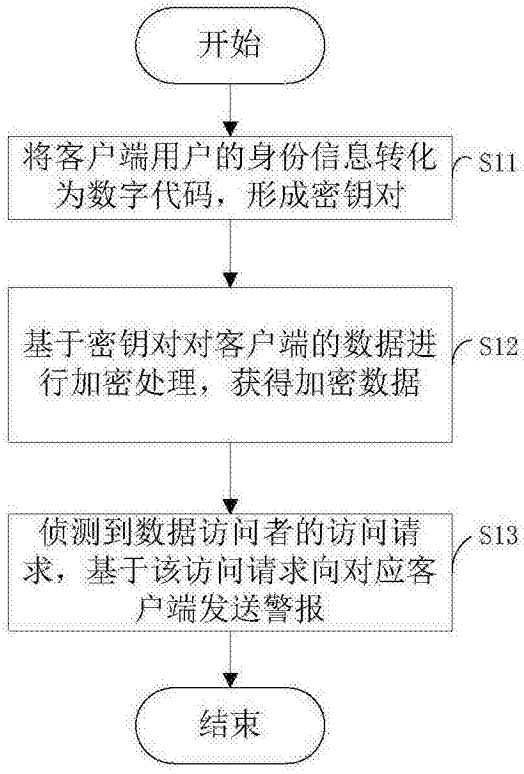

开始
将客户端用户的身份信息转化为数字代码，形成密钥对
S11
基于密钥对对客户端的数据进行加密处理，获得加密数据
S12
侦测到数据访问者的访问请求，基于该访问请求向对应客户端发送警报
S13
结束

图 2

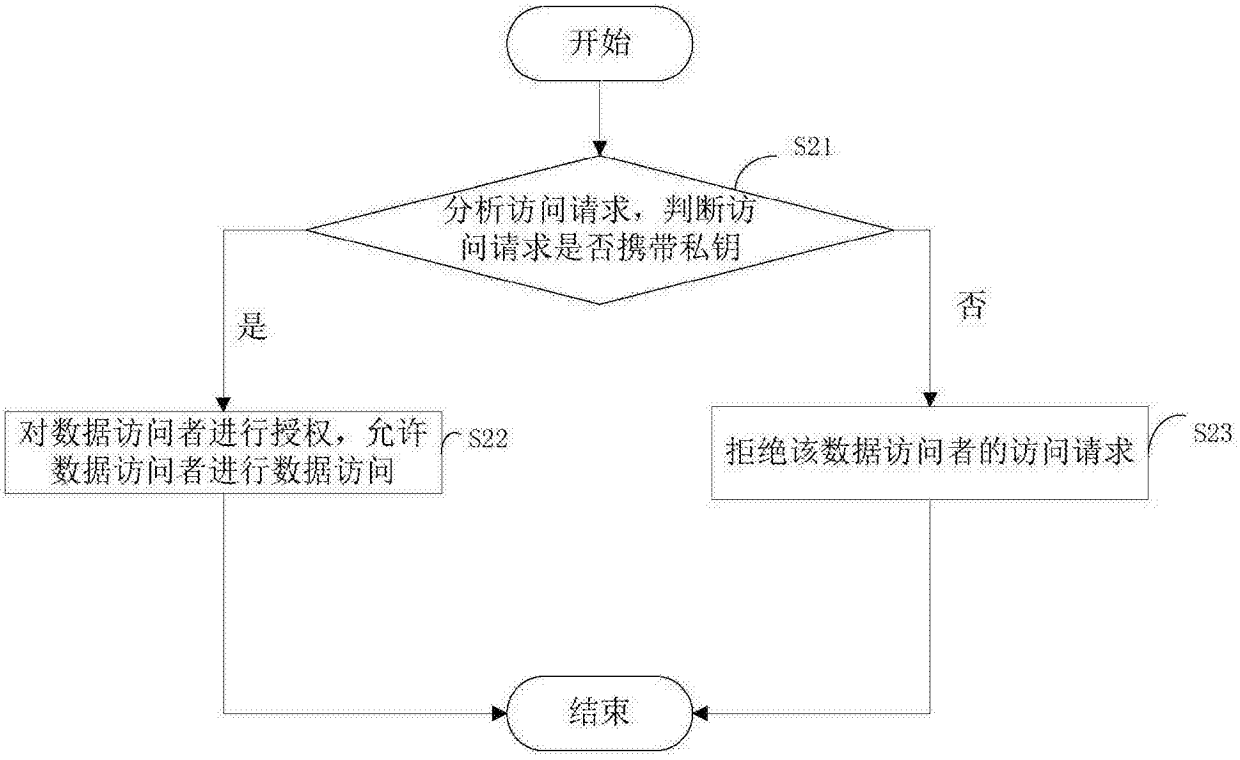

开始
分析访问请求，判断访问请求是否携带私钥
S21
是
否
对数据访问者进行授权，允许数据访问者进行数据访问
S22
拒绝该数据访问者的访问请求
S23
结束

图 3

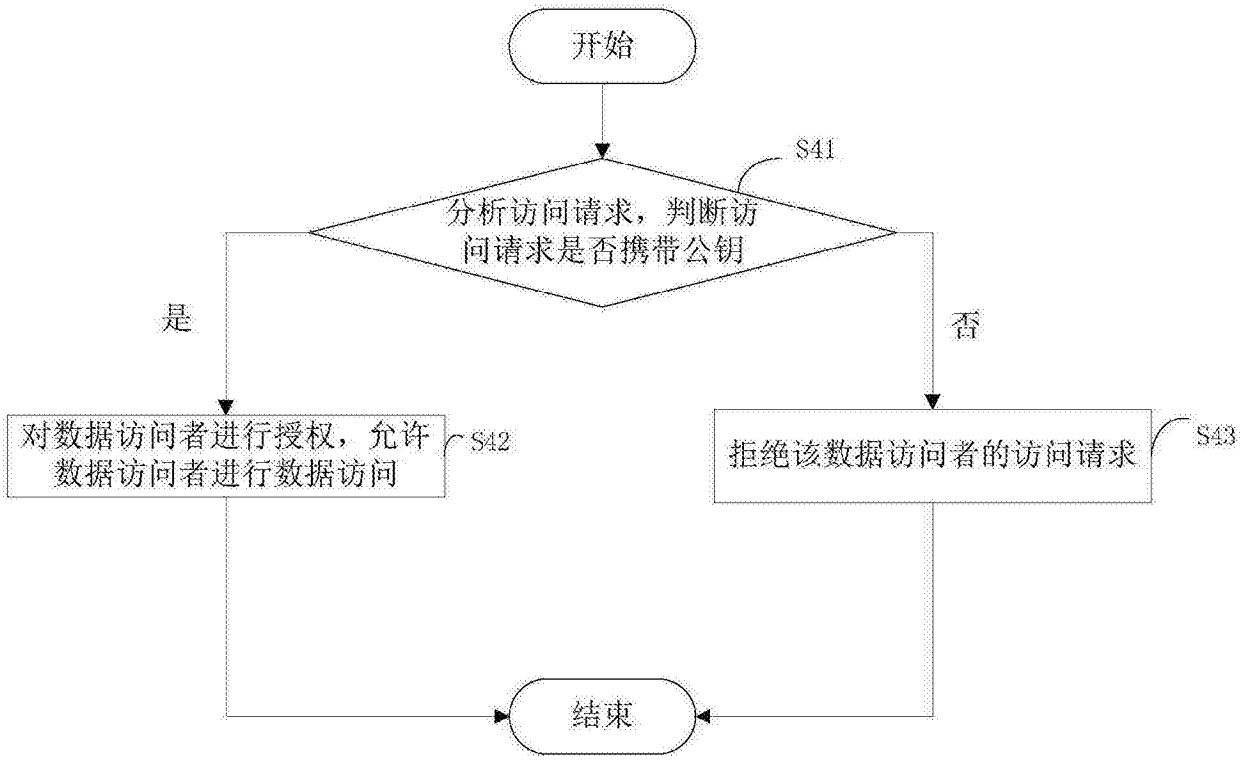

开始
S41
分析访问请求，判断访问请求是否携带公钥
是
否
对数据访问者进行授权，允许数据访问者进行数据访问
S42
拒绝该数据访问者的访问请求
S43
结束

图 4

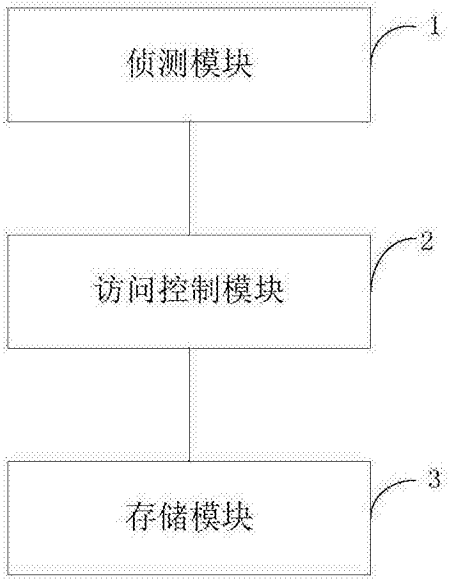

侦测模块
1
访问控制模块
2
存储模块
3

图 5

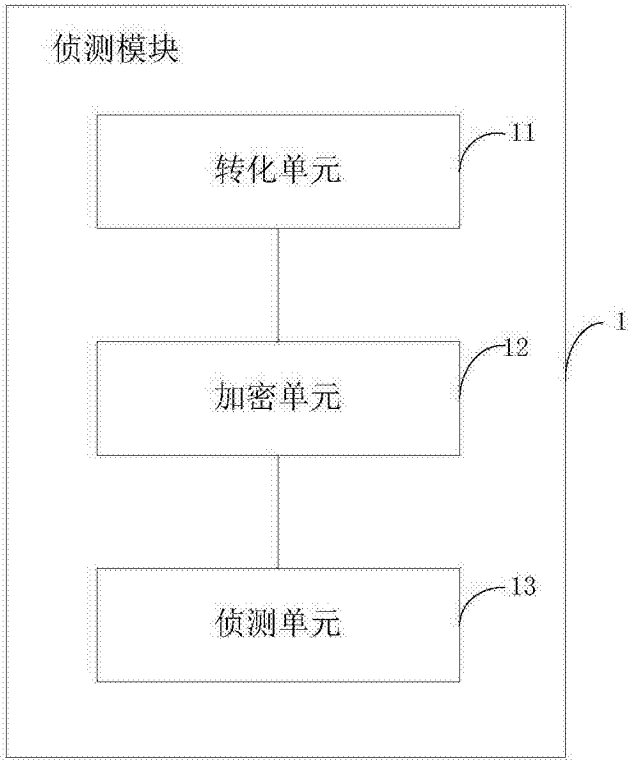

侦测模块
转化单元
11
加密单元
12
侦测单元
13
1

图 6

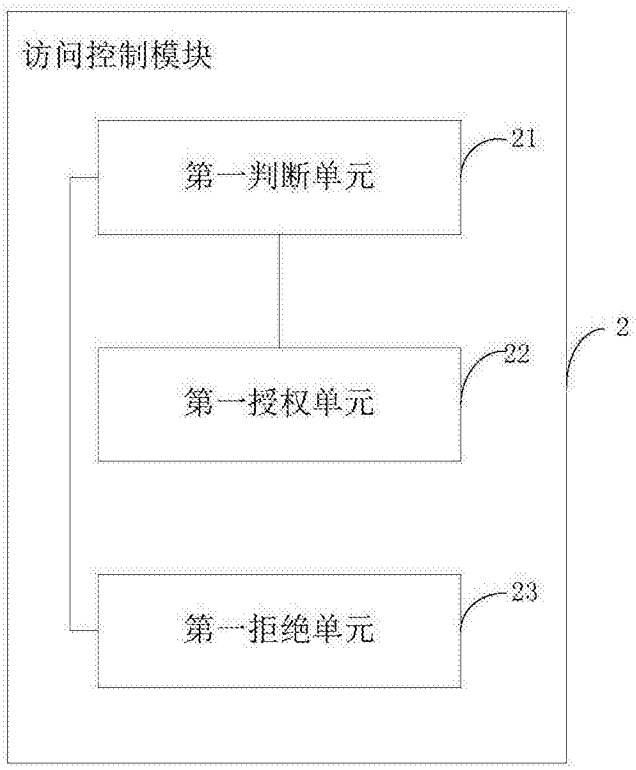

访问控制模块
第一判断单元
21
第一授权单元
22
2
第一拒绝单元
23

图 7

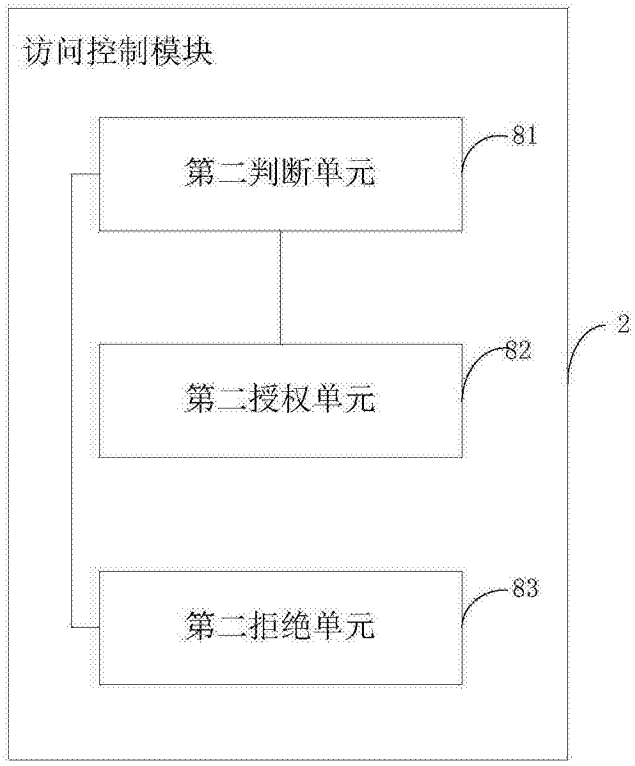

访问控制模块
第二判断单元
81
第二授权单元
82
2
第二拒绝单元
83

图 8