(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116527365 A
(43)申请公布日 2023.08.01

(21)申请号 202310513128.7

(22)申请日 2023.05.08

(71)申请人 清华大学
地址 100084 北京市海淀区清华园
申请人 中国民用航空局空中交通管理局

(72)发明人 张毅 何泓霖 晏松 韩少聪
杨敬轩 陈宝刚 杨锐

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
专利代理师 李丹 栗若木

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

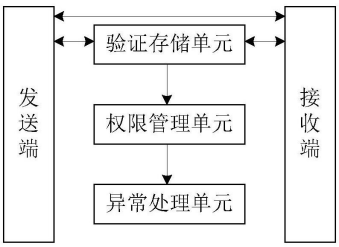
权利要求书2页 说明书8页 附图3页

(54)发明名称

实现空管异构数据共享的系统及方法

(57)摘要

本文公开一种实现空管异构数据共享的系统及方法，包括：系统的发送端设置为：签名处理原始数据，获得第一数据；将第一数据和第一密钥分别进行对称加密，获得第二数据和第二密钥；将第二密钥通过来自接收端的公钥进行加密，获得第三密钥；发送第二数据和第三密钥至接收端；系统的接收端设置为：在本地存储生成的公钥和私钥中的私钥，发送公钥至发送端；通过本地的私钥解密来自发送端的第三密钥，获得第二密钥；利用第二密钥解密来自发送端的第二数据，获得第一数据；签名查验第一数据，获得原始数据；原始数据包括：空管数据。本发明实施例基于混合加密机制进行数据传输处理，保证了空管数据的机密性以及数据源的可验证性。



CN 116527365 A

1.一种实现空管异构数据共享的系统,包括:发送端和接收端;其中,

发送端设置为:对共享的原始数据进行签名处理,获得第一数据;将签名处理获得的第一数据和第一密钥分别进行对称加密,获得第二数据和第二密钥;将获得的第二密钥通过来自接收端的公钥进行加密,获得第三密钥;发送获得的第二数据和第三密钥至接收端;

接收端设置为:将生成的一对公钥和私钥中的私钥在本地存储,发送生成的公钥至发送端;通过本地存储的私钥对来自发送端的第三密钥进行解密,获得第二密钥;利用解密获得的第二密钥对来自发送端的第二数据进行解密,获得第一数据;对解密获得的第一数据进行签名查验,获得原始数据;

其中,所述原始数据包括:空管数据。

2.根据权利要求1所述的系统,其特征在于:

所述发送端还设置为:所述对共享的原始数据进行签名处理之前,通过预设的杂凑加密算法对所述原始数据进行处理,获得第一散列值,发送第一散列值至接收端;

所述接收端还设置为:所述获得原始数据之后,通过所述杂凑加密算法获得所述原始数据进行处理,获得第二散列值;通过比对第一散列值和第二散列值,确定接收到的来自所述发送端的数据是否完整。

3.根据权利要求1所述的系统,其特征在于,所述系统还包括验证存储单元,设置为:

对接收到的待存储的第三数据,判断其数据格式是否与预先设定的标准格式相符;

将与所述标准格式相符的第三数据写入预先设定的数据库中;

对与所述标准格式不相符的第三数据,执行拒绝写入所述数据库的处理。

4.根据权利要求3所述的系统,其特征在于,所述系统还包括权限管理单元,设置为:

存储用于确定用户对所述第三数据的访问权限的身份属性的信息;

接收到用户的访问请求时,根据存储的身份属性的信息为用户提供相应的所述第三数据的访问权限。

5.根据权利要求4所述的系统,其特征在于,所述系统还包括异常处理单元,设置为:

根据用户的访问操作信息确定用户的访问操作是否异常;

确定用户的访问操作异常时,对用户的访问执行异常操作处理;

其中,所述异常操作处理包括:访问告警和/或中断连接处理。

6.根据权利要求5所述的系统,其特征在于,所述异常处理单元是设置为根据用户的访问操作信息确定用户访问操作是否异常,包括:

采用孤立森林模型对所述访问操作信息进行检测,以确定用户访问操作是否异常。

7.一种实现空管异构数据共享的方法,包括:

发送端对共享的原始数据进行签名处理,获得第一数据;

将签名处理获得的第一数据和第一密钥分别进行对称加密,获得第二数据和第二密钥;

接收来自接收端的公钥,并将第二密钥通过接收到的公钥进行加密,获得第三密钥;

将第二数据和第三密钥,发送至接收端;

其中,所述原始数据包括:空管数据。

8.一种实现空管异构数据共享的方法,包括:

接收端生成一对公钥和私钥,并在本地存储私钥,发送公钥至发送端;

接收端接收第三密钥,并通过本地存储的私钥对第三密钥进行解密,获得第二密钥;

利用解密获得的第二密钥对接收到的第二数据进行解密,获得第一数据;

对解密获得的第一数据进行签名查验,获得原始数据;

其中,所述原始数据包括:空管数据。

9.一种计算机存储介质,所述计算机存储介质中存储有计算机程序,所述计算机程序被处理器执行时实现如权利要求7或8所述的实现空管异构数据共享的方法。

10.一种终端,包括:存储器和处理器,所述存储器中保存有计算机程序;其中,

处理器被配置为执行存储器中的计算机程序;

所述计算机程序被所述处理器执行时实现如权利要求7或8所述的实现空管异构数据共享的方法。

实现空管异构数据共享的系统及方法

技术领域

[0001] 本文涉及但不限于数据安全技术，尤指一种实现空管异构数据共享的系统及方法。

背景技术

[0002] 在当前信息化的时代背景下，数据信息成为了重要的社会资源；同时，为了信息系统的可持续发展，促进企业间合作共赢，企业间数据共享就逐渐成为了一项不可或缺的重要事务。我国数据安全的相关法律指出，国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展；开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

[0003] 面对日益发展的信息化趋势，空管系统也不可避免地将与外界产生交互，空管系统现有及未来可预见的一段时期内的数据引接和数据共享需求将会不断增多。空管系统的信息具有敏感性，数据安全级别相对较高，用于数据共享的系统必须具有极高的安全性，需要满足跨平台、可扩展、可追溯、权责明确的要求，同时数据的安全共享还不能影响现有系统的正常运行。

[0004] 基于民航空管数据安全特性，考虑数据遭到篡改、破坏、泄露或者非法获取、非法利用，可能对国家安全、公共利益或者个人、组织合法权益造成的危害，在满足空管数据引接和共享需求的前提下，基于空管现有及未来可预见的一段时期的数据共享需求，结合国家关键信息基础设施和网络安全等级保护相关要求，结合民航空管数据中心总体建设规划以及打造一个“统一的网络安全防护体系”的目标，参考国内外网络安全数据共享方法，构建一套数据安全的保障系统，成为一个有待解决的问题。

发明内容

[0005] 以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

[0006] 本发明实施例提供一种实现空管异构数据共享的系统及方法，能够保障空管数据的传输和应用。

[0007] 本发明实施例提供了一种实现空管异构数据共享的系统，包括：发送端和接收端；其中，

[0008] 发送端设置为：对共享的原始数据进行签名处理，获得第一数据；将签名处理获得的第一数据和第一密钥分别进行对称加密，获得第二数据和第二密钥；将获得的第二密钥通过来自接收端的公钥进行加密，获得第三密钥；发送获得的第二数据和第三密钥至接收端；

[0009] 接收端设置为：将生成的一对公钥和私钥中的私钥在本地存储，发送生成的公钥

至发送端;通过本地存储的私钥对来自发送端的第三密钥进行解密,获得第二密钥;利用解密获得的第二密钥对来自发送端的第二数据进行解密,获得第一数据;对解密获得的第一数据进行签名查验,获得原始数据;

[0010] 其中,所述原始数据包括:空管数据。

[0011] 另一方面,本发明实施例还提供一种实现空管异构数据共享的方法,包括:

[0012] 发送端对共享的原始数据进行签名处理,获得第一数据;

[0013] 将签名处理获得的第一数据和第一密钥分别进行对称加密,获得第二数据和第二密钥;

[0014] 接收来自接收端的公钥,并将第二密钥通过接收到的公钥进行加密,获得第三密钥;

[0015] 将第二数据和第三密钥,发送至接收端;

[0016] 其中,所述原始数据包括:空管数据。

[0017] 还一方面,本发明实施例还提供一种计算机存储介质,所述计算机存储介质中存储有计算机程序,所述计算机程序被处理器执行时实现上述实现空管异构数据共享的方法。

[0018] 还一方面,本发明实施例还提供一种终端,包括:存储器和处理器,所述存储器中保存有计算机程序;其中,

[0019] 处理器被配置为执行存储器中的计算机程序;

[0020] 所述计算机程序被所述处理器执行时实现如上述实现空管异构数据共享的方法。

[0021] 还一方面,本发明实施例还提供一种实现空管异构数据共享的方法,包括:

[0022] 接收端生成一对公钥和私钥,并在本地存储私钥,发送公钥至发送端;

[0023] 接收端接收第三密钥,并通过本地存储的私钥对第三密钥进行解密,获得第二密钥;

[0024] 利用解密获得的第二密钥对接收到的第二数据进行解密,获得第一数据;

[0025] 对解密获得的第一数据进行签名查验,获得原始数据;

[0026] 其中,所述原始数据包括:空管数据。

[0027] 还一方面,本发明实施例还提供一种计算机存储介质,所述计算机存储介质中存储有计算机程序,所述计算机程序被处理器执行时实现上述实现空管异构数据共享的方法。

[0028] 还一方面,本发明实施例还提供一种终端,包括:存储器和处理器,所述存储器中保存有计算机程序;其中,

[0029] 处理器被配置为执行存储器中的计算机程序;

[0030] 所述计算机程序被所述处理器执行时实现如上述实现空管异构数据共享的方法。

[0031] 本申请技术方案中的系统,包括:发送端和接收端;其中,发送端设置为:对共享的原始数据进行签名处理,获得第一数据;将签名处理获得的第一数据和第一密钥分别进行对称加密,获得第二数据和第二密钥;将获得的第二密钥通过来自接收端的公钥进行加密,获得第三密钥;发送获得的第二数据和第三密钥至接收端;接收端设置为:将生成的一对公钥和私钥中的私钥在本地存储,发送生成的公钥至发送端;通过本地存储的私钥对来自发送端的第三密钥进行解密,获得第二密钥;利用解密获得的第二密钥对来自发送端的第二

数据进行解密，获得第一数据；对解密获得的第一数据进行签名查验，获得原始数据；其中，原始数据包括：空管数据。本发明实施例基于混合加密机制进行数据传输处理，保证了空管数据的机密性以及数据源的可验证性。

[0032] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0033] 附图用来提供对本发明技术方案的进一步理解，并且构成说明书的一部分，与本申请的实施例一起用于解释本发明的技术方案，并不构成对本发明技术方案的限制。

[0034] 图1为本发明实施例实现空管异构数据共享的系统的结构框图

[0035] 图2为本发明实施例一实现空管异构数据共享的方法的流程图；

[0036] 图3为本发明实施例另一实现空管异构数据共享的方法的流程图；

[0037] 图4为本发明应用示例实现空管异构数据共享的系统的示意图；

[0038] 图5为本发明应用示例基于混合加密机制的数据传输网络示意图；

[0039] 图6为本应用示例进行异常行为处理的流程图。

具体实施方式

[0040] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0041] 在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行。并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0042] 图1为本发明实施例实现空管异构数据共享的系统的结构框图，如图1所示，包括：发送端和接收端；其中，

[0043] 发送端设置为：对共享的原始数据进行签名处理，获得第一数据；将签名处理获得的第一数据和第一密钥分别进行对称加密，获得第二数据和第二密钥；将获得的第二密钥通过来自接收端的公钥进行加密，获得第三密钥；发送获得的第二数据和第三密钥至接收端；

[0044] 接收端设置为：将生成的一对公钥和私钥中的私钥在本地存储，发送生成的公钥至发送端；通过本地存储的私钥对来自发送端的第三密钥进行解密，获得第二密钥；利用解密获得的第二密钥对来自发送端的第二数据进行解密，获得第一数据；对解密获得的第一数据进行签名查验，获得原始数据；

[0045] 其中，原始数据包括：空管数据。

[0046] 本发明实施例基于混合加密机制进行数据传输处理，保证了空管数据的机密性以及数据源的可验证性。

[0047] 在一种示例性实例中，本发明实施例中的：发送端还设置为：对共享的原始数据进行签名处理之前，通过预设的杂凑加密算法对原始数据进行处理，获得第一散列值，发送第

一散列值至接收端;接收端还设置为:获得原始数据之后,通过杂凑加密算法获得原始数据进行处理,获得第二散列值;通过比对第一散列值和第二散列值,确定接收到的来自发送端的数据是否完整。

[0048] 本发明实施例通过上述处理,实现了传输的数据的完整性验证,保证了数据传输的安全性。

[0049] 在一种示例性实例中,本发明实施例系统还包括验证存储单元,设置为:

[0050] 对接收到的待存储的第三数据,判断其数据格式是否与预先设定的标准格式相符;

[0051] 将与标准格式相符的第三数据写入预先设定的数据库中;

[0052] 对与标准格式不相符的第三数据,执行拒绝写入数据库的处理。

[0053] 在一种示例性实例中,本发明实施例系统还包括权限管理单元,设置为:

[0054] 存储用于确定用户对第三数据的访问权限的身份属性的信息;

[0055] 接收到用户的访问请求时,根据存储的身份属性的信息为用户提供相应的第三数据的访问权限。

[0056] 在一种示例性实例中,本发明实施例系统还包括异常处理单元,设置为:

[0057] 根据用户的访问操作信息确定用户的访问操作是否异常;

[0058] 确定用户的访问操作异常时,对用户的访问执行异常操作处理;

[0059] 其中,异常操作处理包括:访问告警和/或中断连接处理。

[0060] 在一种示例性实例中,本发明实施例异常处理单元是设置为根据用户的访问操作信息确定用户访问操作是否异常,包括:

[0061] 采用孤立森林模型对访问操作信息进行检测,以确定用户访问操作是否异常。在一种示例性实例中,本发明实施例验证存储单元、权限管理单元和异常处理单元,可以是对空管数据进行存储和管理的服务器中的组成单元,可以由本领域技术人员参照系统工作原理进行设计实现。

[0062] 图2为本发明实施例一实现空管异构数据共享的方法的流程图,如图2所示,包括:

[0063] 步骤201、发送端对共享的原始数据进行签名处理,获得第一数据;

[0064] 步骤202、将签名处理获得的第一数据和第一密钥分别进行对称加密,获得第二数据和第二密钥;

[0065] 步骤203、接收来自接收端的公钥,并将第二密钥通过接收到的公钥进行加密,获得第三密钥;

[0066] 步骤204、将第二数据和第三密钥,发送至接收端;

[0067] 其中,原始数据包括:空管数据。

[0068] 本发明实施例还提供一种计算机存储介质,计算机存储介质中存储有计算机程序,计算机程序被处理器执行时实现上述实现空管异构数据共享的方法。

[0069] 本发明实施例还提供一种终端,包括:存储器和处理器,存储器中保存有计算机程序;其中,

[0070] 处理器被配置为执行存储器中的计算机程序;

[0071] 计算机程序被处理器执行时实现如上述实现空管异构数据共享的方法。

[0072] 图3为本发明实施例另一实现空管异构数据共享的方法的流程图,如图3所示,包

括：

[0073] 步骤301、接收端生成一对公钥和私钥，并在本地存储私钥，发送公钥至发送端；

[0074] 步骤302、接收端接收第三密钥，并通过本地存储的私钥对第三密钥进行解密，获得第二密钥；

[0075] 步骤303、利用解密获得的第二密钥对接收到的第二数据进行解密，获得第一数据；

[0076] 步骤304、对解密获得的第一数据进行签名查验，获得原始数据；

[0077] 其中，原始数据包括：空管数据。

[0078] 本发明实施例还提供一种计算机存储介质，计算机存储介质中存储有计算机程序，计算机程序被处理器执行时实现上述实现空管异构数据共享的方法。

[0079] 本发明实施例还提供一种终端，包括：存储器和处理器，存储器中保存有计算机程序；其中，

[0080] 处理器被配置为执行存储器中的计算机程序；

[0081] 计算机程序被处理器执行时实现如上述实现空管异构数据共享的方法。

[0082] 以下通过应用示例对本发明实施例进行简要说明，应用示例仅用于陈述本发明实施例，并不用于限定本发明的保护范围。

[0083] 应用示例

[0084] 图4为本发明应用示例实现空管异构数据共享的系统的示意图，如图4所示，本应用示例数据处理包括三个部分：数据提供者、数据使用者和信息共享环境；包括数据平面和控制平面的数据交互。

[0085] 在数据平面，本应用示例按照预设格式对数据(存储在信息共享环境中的数据，包括本发明实施例中的第三数据)进行整理；按照预设的权限，为不同种类数据分别设置相应的访问权限；接收到用户的访问请求时，为用户根据其访问权限输出相应的数据；在一种示例性实例中，本应用示例在数据平面，数据的提供者需要将共享数据打包成预设格式后，再传递至共享环境。传递到共享环境中的数据标注了访问权限的权限属性信息，即不同数据的共享对象要求的身份属性。共享环境提供信息接收服务，接收数据提供者传送的数据，并存入数据库；同时面向使用者提供数据读取的服务，接收来自使用者的读取请求，根据使用者的身份属性判断用户对数据的访问权限，根据判断结果发送数据给使用者。本应用示例基于访问权限管理，能够实现多种形式的信息的检索功能，接收数据使用者的读取请求，实现对数据的检索和读取，并将数据反馈给使用者。

[0086] 在控制平面，本应用示例预先存储不同用户的身份属性的信息，身份属性的信息可以用于确定用户对数据的访问权限；根据存储的身份属性的信息，确定用户对数据的访问权限；通过确定的用户的访问权限，为用户提供相应的访问数据的权限；进一步的，根据捕获的用户的访问操作信息，确定访问操作是否异常，判断出访问操作异常时，执行访问告警和/或对用户执行中断连接处理。在一种示例性实例中，本应用示例在开放数据接收服务给信息提供者之前，共享环境需要从多角度收集信息，验证信息提供者的身份，并根据一定的策略，决定是否授权建立相应的数据通信的连接；数据连接建立后，共享环境需要持续地跟踪和评估通信的行为，并判决用户的操作是否符合行为规则，一旦发现访问操作异常，需要采取对应的异常操作处理。同样，对于使用数据的用户，共享环境在开放数据读取服务

前，需要验证用户的身份，并在数据读取过程中持续分析访问操作信息，以确定是否中断服务，以保护数据不被非法获取。

[0087] 本应用示例基于民航空管数据安全特性，考虑数据遭到篡改、破坏、泄露、非法获取或者非法利用，对国家安全、公共利益、个人或组织合法权益造成的危害，在满足空管数据引接和共享需求的前提下，构建数据安全的访问处理方法。针对空管业务系统，针对数据传输和访问的各个部分分别设计了安全保障机制，确立了系统的输入输出引接方式，兼具系统性、完整性和安全性。

[0088] 在一种示例性实例中，本应用示例处理包括：对接收到的数据，根据是否与标准格式相符的判断，执行数据是否写入数据库的处理；本应用示例预先设定系统接收的数据的标准格式，接收到数据后，按照标准格式对接收的数据进行格式验证，将通过格式验证的数据写入数据库中，对未通过格式验证的数据，拒绝其写入数据库的请求。

[0089] 在一种示例性实例中，本应用示例提供端到端的安全传输的加密通道，采用一次一密和数字签名机制，保证数据传输过程中即使被第三方截获，也不会被窃取、篡改和伪造，从而保证了数据的机密性、完整性和不可否认性。

[0090] 图5为本发明应用示例基于混合加密机制的数据传输网络示意图，如图5所示，在数据传输过程中，需要发送端与接收端协议商定非对称加密密钥，即接收端生成一对公钥和私钥，并向发送端公开公钥，接收端负责维护私钥。

[0091] 在数据共享的过程中，发送端首先进行数据签名处理，将签名处理的数据和密钥分别进行对称加密，发送对称加密后的数据接收端；同时，将对称加密的密钥通过来自接收端的公钥加密后，发送给接收端。

[0092] 接收端接收到加密后的对称密钥后，通过预先存储的与公钥对应的私钥对加密的对称密钥进行解密，获得对称加密的密钥；利用解密获得的对称加密的密钥对接收到的加密数据进行解密；对解密获得的数据进行签名查验，获得原始数据。

[0093] 本发明实施例基于上述混合加密机制进行数据传输，保证了数据的机密性以及数据源的可验证性。

[0094] 在一种示例性实例中，本应用示例方法还包括：在传输数据之前，发送端通过预设的杂凑加密算法对传输的数据进行处理，获得第一散列值；

[0095] 接收端通过杂凑加密算法对接收到数据进行处理，获得第二散列值；

[0096] 通过比对第一散列值和第二散列值，确定传输的数据是否完整。

[0097] 在一种示例性实例中，本应用示例中的杂凑加密算法包括：SM3杂凑算法。

[0098] 在一种示例性实例中，本应用示例方法还包括：通过预先存储的用户信息，对用户身份进行验证，根据预设的一种以上不同用户的用户信息，为登录的用户提供预先设定的访问权限；在一种示例性实例中，本应用示例基于以下一种以上用户信息为登录用户提供预先设定的访问权限：用户账号、设备型号、设备配置、软件版本和操作系统等；本应用示例可以接收外部多来源的用户信息，结合身份验证结果执行访问权限控制；同时对于授权的数据存取行为，进行跟踪监视。

[0099] 在一种示例性实例中，本应用示例对具有访问权限的用户，通过生成具体会话的身份验证令牌或凭证，供客户端与服务建立会话。本应用示例如果会话被授权且请求通过身份验证，将允许会话启动；如果会话被拒绝，则通过预设信号切断会话连接。

[0100] 在一种示例性实例中，本应用示例方法还包括：对已经建立的通信连接，进行流量的异常行为分析；并将分析结果反馈给策略引擎。本应用示例通过异常行为分析，可以阻止一部分仿冒合法用户身份的异常数据访问行为，比如非工作时间大量访问敏感数据等。在一种示例性实例中，本应用示例可以按照预设周期收集用户的上下行流量，利用相关技术中异常检测方法对收集的上下行流量进行分析，以实现异常行为的检测。

[0101] 在一种示例性实例中，本应用示例采用孤立森林模型检测当前时刻所有参与数据共享的用户，确定用户的行为是否异常；在一种示例性实例中，通过孤立森林模型对用户进行异常行为分析包括：从用户登录起即对用户行为进行实时检测，判断用户行为是否异常；包括但不限于：上下文异常。每个孤立森林模型所输出的都是一个异常值得分，图6为本应用示例进行异常行为处理的流程图，如图6所示，当用户自登录以来的异常值得分达到预先设定的阈值时，判定用户行为异常，此时可以认为当前用户身份不可信，对用户访问数据的行为可以进行中断连接处理。

[0102] 在一种示例性实例中，本应用示例孤立森林模型的输入为：固定时刻下所有用户的流量；在一种示例性实例中，本应用根据数据共享过程的基本特点，兼顾辨识效率和准确性等因素，选择如：用户登录时刻、用户在当前检测时刻和上一检测时刻等时间段内的上下行流量、用户自登录以来的上下行流量总量等特征项。在一种示例性实例中，本应用示例孤立森林模型的输出为：固定时刻下每个用户的异常值得分，得分值在0-1之间，若异常值得分大于预设的阈值时(例如大于0.9)，则认为对应用户在当期时刻行为存在异常；若异常值得分趋近于0.5，则认为用户不存在异常。本应用示例每一用户自登录时，初始化异常值得分S为0，在每一时刻，利用孤立森林模型确定其异常值得分，若异常值超过阈值d，则其累积异常值得分S相应增加d，当S超过一阈值K时，采取阻断措施；其中，d和K由本领域技术人员根据历史数据的特征结合经验设定的参数。

[0103] 在一种示例性实例中，本应用示例方法还包括记录以下一项或任意组合的信息：主机执行的命令、传输的数据、通信双方的地址、通信端口等信息。在一种示例性实例中，本应用示例参照相关技术对上述方法记录的信息和/或日志信息进行存储，以防止数据被随意的删改。

[0104] 本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些组件或所有组件可以被实施为由处理器，如数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模

块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据,并且可包括任何信息递送介质。

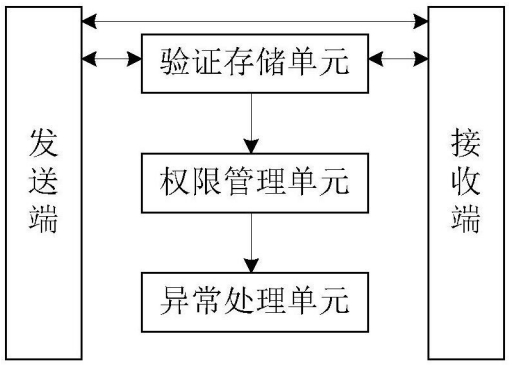

发送端
验证存储单元
权限管理单元
异常处理单元
接收端

图1

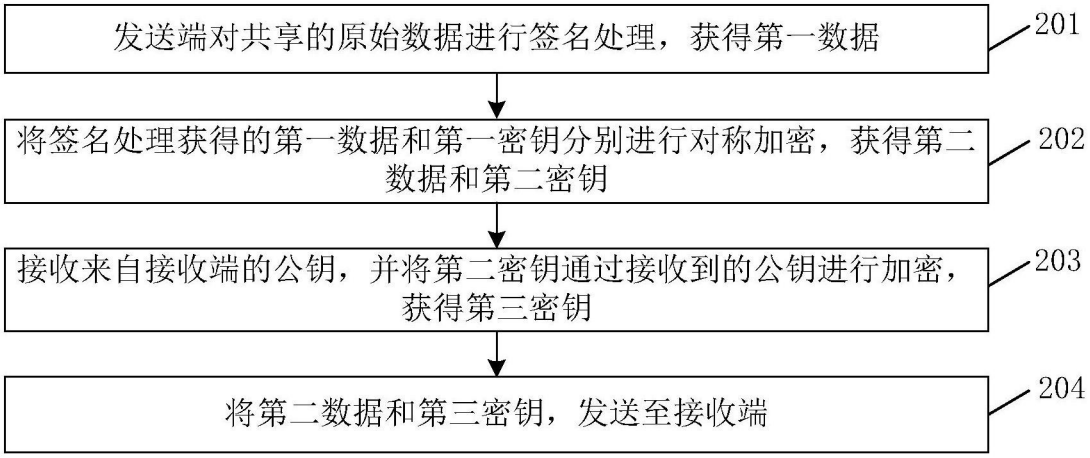

发送端对共享的原始数据进行签名处理，获得第一数据
201
将签名处理获得的第一数据和第一密钥分别进行对称加密，获得第二数据和第二密钥
202
接收来自接收端的公钥，并将第二密钥通过接收到的公钥进行加密，获得第三密钥
203
将第二数据和第三密钥，发送至接收端
204

图2

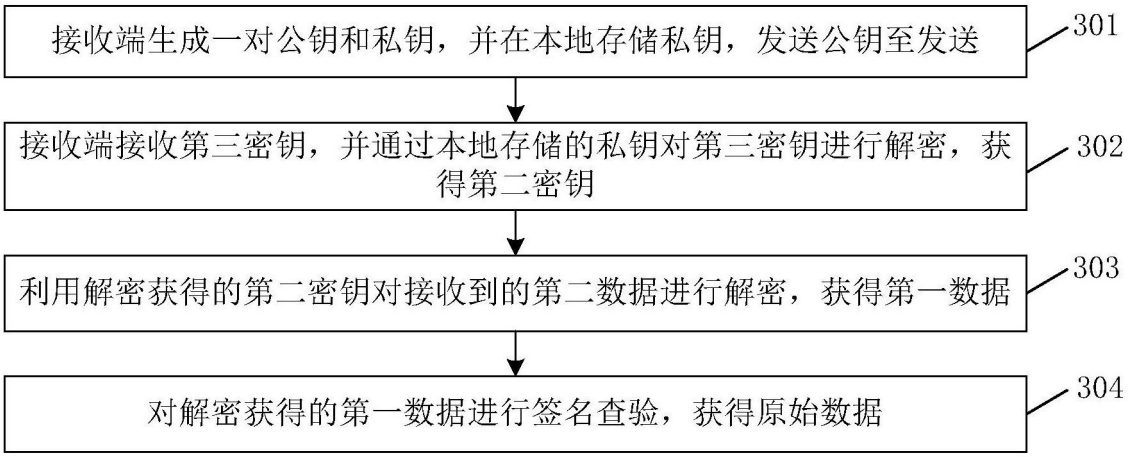

接收端生成一对公钥和私钥，并在本地存储私钥，发送公钥至发送
301
接收端接收第三密钥，并通过本地存储的私钥对第三密钥进行解密，获得第二密钥
302
利用解密获得的第二密钥对接收到的第二数据进行解密，获得第一数据
303
对解密获得的第一数据进行签名查验，获得原始数据
304

图3

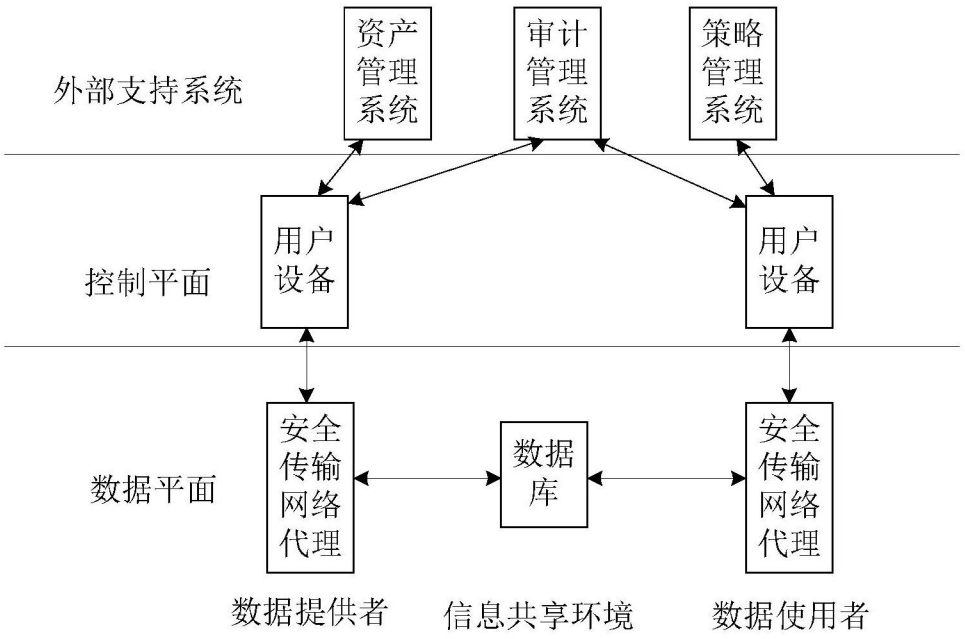

外部支持系统
资产管理系统
审计管理系统
策略管理系统
控制平面
用户设备
用户设备
数据平面
安全传输网络代理
数据库
安全传输网络代理
数据提供者
信息共享环境
数据使用者

图4

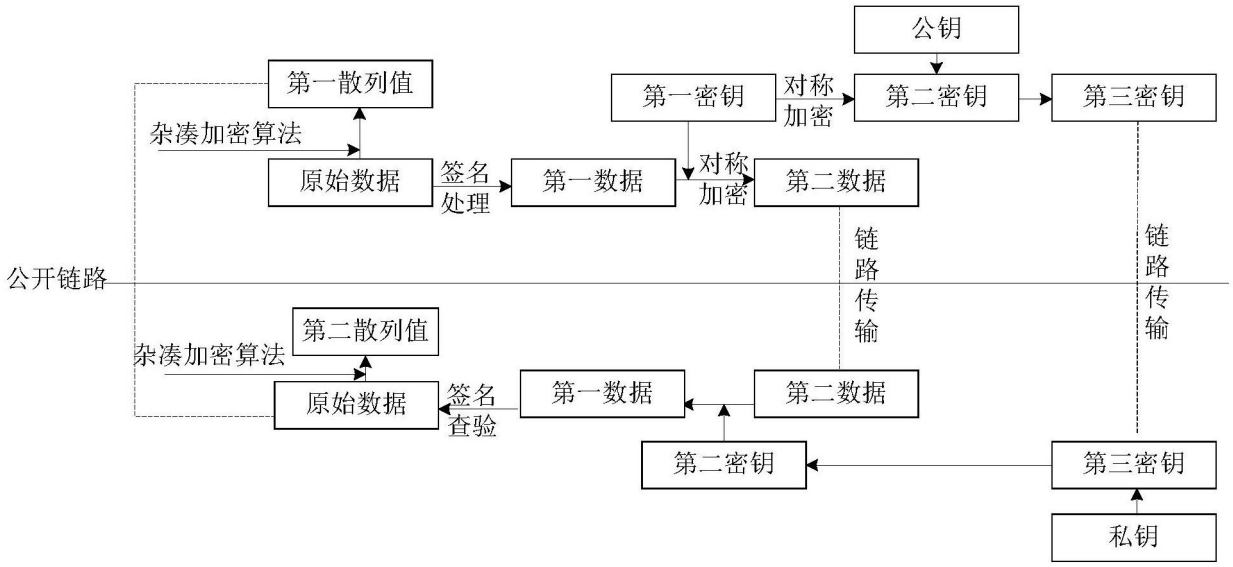

公钥
第一密钥
对称加密
第二密钥
第三密钥
第一散列值
杂凑加密算法
原始数据
签名处理
第一数据
对称加密
第二数据
链路传输
链路传输
公开链路
第二散列值
杂凑加密算法
原始数据
签名查验
第一数据
第二数据
第二密钥
第三密钥
私钥

图5

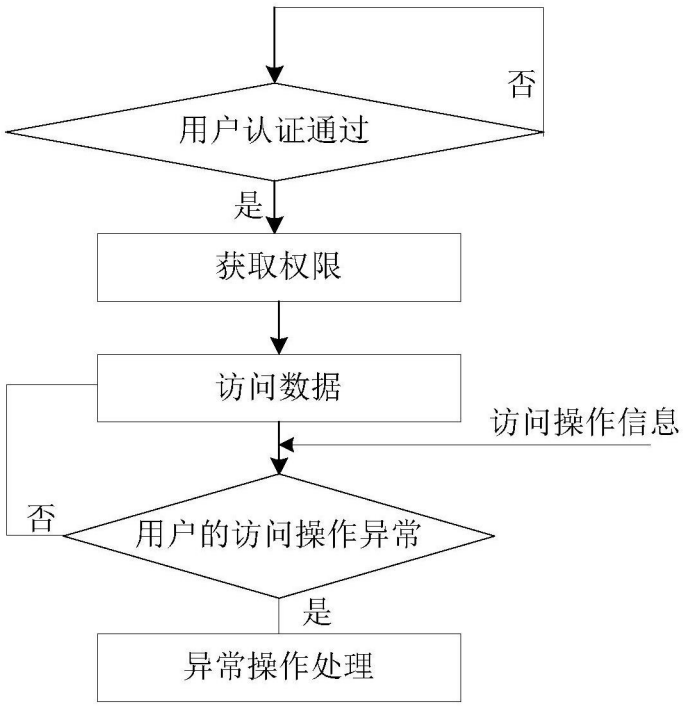


图6