(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 101860548 A
(43)申请公布日 2010.10.13

(21)申请号 201010209178.9

(22)申请日 2010.06.17

(71)申请人 北京握奇数据系统有限公司
地址 100015 北京市朝阳区东直门外西八间房万红西街 2 号燕东商务花园

(72)发明人 高翔 关宇

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 郭润湘

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

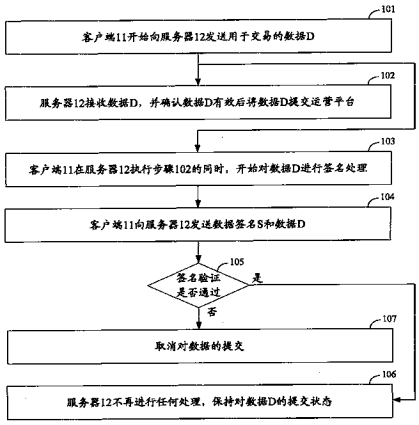
权利要求书 1 页 说明书 5 页 附图 3 页

(54)发明名称

一种数据签名验证的方法、装置及系统

(57)摘要

为了解决基于数据签名验证过程数据安全性得到保证的前提下，数据有效性的确认时间较长的问题，本发明公开了一种数据签名验证的方法、装置及系统，该方法包括：服务器接收客户端发送的数据和数据签名，确认数据有效后将数据提交运营平台，对数据签名进行验证，若数据签名验证成功，则维持数据的提交状态，否则，撤销所述数据的提交，由于当数据签名验证和将数据提交运营平台并行处理，使得基于数据签名验证过程数据安全性得到保证的前提下，减短了数据提交运营平台的时间。



CN 101860548 A

1. 一种数据签名验证的方法，其特征在于，包括：

服务器接收客户端发送的数据和数据签名；

服务器确认所述数据有效后将所述数据提交运营平台；

服务器对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

2. 如权利要求 1 所述的方法，其特征在于，确认所述数据有效后，若预定时间内服务器没有收到数据签名，则撤销所述数据的提交。

3. 如权利要求 1 所述的方法，其特征在于，服务器确认所述数据有效具体为：

服务器在客户端对数据进行签名处理的同时，接收客户端发送的数据并确认数据有效；

或者，

客户端对数据进行签名处理后，服务器接收客户端发送的数据，服务器在对数据签名进行验证的同时，对数据的有效性进行确认。

4. 如权利要求 1 所述的方法，其特征在于，所述服务器接收客户端发送数据和的数据签名步骤具体为：

服务器接收数据以及包含所述数据和数据签名的数据包。

5. 一种数据签名验证的装置，其特征在于，包括：

接收模块，用于接收客户端发送的数据和数据签名；

数据确认模块，用于确认所述数据有效后将所述数据提交运营平台；

数据验证模块，用于对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

6. 如权利要求 5 所述的装置，其特征在于，数据验证模块，还用于确认所述数据有效后，若预定时间内没有收到数据签名，则撤销所述数据的提交。

7. 如权利要求 5 所述的装置，其特征在于，数据确认模块，还用于在客户端对数据进行签名处理的同时，接收客户端发送的数据并确认数据有效，或者，客户端对数据进行签名处理后，接收客户端发送的数据，在对数据签名进行验证的同时，对数据的有效性进行确认。

8. 如权利要求 5 所述的装置，其特征在于，接收模块，还用于接收数据以及包含所述数据和数据签名的数据包。

9. 一种数据签名验证的系统，其特征在于，包括：

客户端，用于向服务器发送数据和数据签名；

服务器，用于接收客户端发送的数据和数据签名，确认所述数据有效后将所述数据提交运营平台，对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

10. 如权利要求 9 所述的系统，其特征在于，客户端，还用于向服务器发送数据以及包含所述数据和数据签名的数据包。

一种数据签名验证的方法、装置及系统

技术领域

[0001] 本发明属于信息处理技术领域，特别涉及一种数据签名验证的方法、装置及系统。

背景技术

[0002] 随着因特网的普及，人们通过因特网进行沟通越来越多，相应的通过网络进行商务活动也变得越来越普及，人们开始广泛的通过网络进行电子商务如在网上购物、进行网上证券交易。然而随着电子商务的飞速发展也相应的引发出一些 Internet 安全问题。基于网络的犯罪活动和木马程序泛滥已经影响到电子商务和网上证券交易系统的安全。考虑到这些风险的存在，目前广泛采用 PKI(Public Key Infrastructure- 公钥基础设施）解决方案来保证电子商务的安全性。除了采用服务器 SSL 安全认证证书来保证服务端的身份安全性以外，部分电子商务系统也开始加强客户端的安全保护，为了保证用户的在系统中提交订单的真实性，引入了客户端数字证书的方式对交易所需的数据进行数字签名，该签名发送给服务端进行验证，验证通过后系统确认该数据有效性并将该数据挂到系统后台。

[0003] 对一些实时性要求较高的电子商务系统如网上证券交易系统，券商以及用户在关注交易的安全性的同时，还会关注的是客户端发送交易所需的数据和系统确认该数据的时间，即当用户提交股票订单和交易系统确认该订单挂单成功的这个时间效率。一般的证券交易系统中，用户提交股票订单和获得确认反馈的时间为 100-200ms，再加上客户端证书签名的保护流程，将会使得整个订单确认时间达到约 150-350ms 时间较长，因此现有技术中存在问题如下 ：基于数据签名验证过程数据安全性得到保证的前提下，数据有效性的确认时间较长。

发明内容

[0004] 为了解决基于数据签名验证过程数据安全性得到保证的前提下，数据有效性的确认时间较长的问题，本发明实施例提供了一种数据签名验证的方法，包括 ：

[0005] 服务器接收客户端发送的数据和数据签名 ；

[0006] 服务器确认所述数据有效后将所述数据提交运营平台 ；

[0007] 服务器对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

[0008] 同时本发明实施例还提供一种数据签名验证的装置，包括 ：

[0009] 接收模块，用于接收客户端发送的数据和数据签名 ；

[0010] 数据确认模块，用于确认所述数据有效后将所述数据提交运营平台 ；

[0011] 数据验证模块，用于对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

[0012] 同时本发明实施例还提供一种数据签名验证的系统，包括 ：

[0013] 客户端，用于向服务器发送数据和数据签名 ；

[0014] 服务器，用于接收客户端发送的数据和数据签名，确认所述数据有效后将所述数

据提交运营平台，对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

[0015] 由上述本发明提供的具体实施方案可以看出，正是由于当数据签名验证成功时，维持数据的提交状态，使得基于数据签名验证过程数据安全性得到保证的前提下，减短了确认数据有效后提交运营平台的时间。

附图说明

[0016] 图 1 为本发明提供的运行第一实施例方法流程图；

[0017] 图 2 为本发明提供的运行第二实施例方法流程图；

[0018] 图 3 为本发明提供的第三实施例装置结构图；

[0019] 图 4 为本发明提供的第四实施例系统结构图。

具体实施方式

[0020] 本发明第一实施例提供了一种数据签名验证的方法，该一种数据签名验证的方法要解决的技术问题是确认数据有效后提交运营平台时间较长，下面以一个证券交易系统为例进行说明，该证券交易系统包括用户的客户端 11 和证券公司的服务器 12，客户端 11 和服务器 12 通过网络连接，服务器 12 接收客户端 11 发送的数据 D 和数据签名 S，服务器 12 接收客户端 11 发送的数据 D，并确认数据 D 有效后将数据 D 提交运营平台这一过程，和客户端 11 产生数据签名 S，服务器 12 对数据签名 S 进行验证这一过程同步进行，本方案关键在于若数据签名 D 验证成功，则保持对没有经过签名验证就直接对数据 D 进行的有效性确认，即维持数据 D 的提交状态，否则，撤销数据 D 的提交。该方法如图 1 所示，具体包括以下步骤：

[0021] 步骤 101：客户端 11 开始向服务器 12 发送用于交易的数据 D。

[0022] 步骤 102：服务器 12 接收数据 D，并确认数据 D 有效后将数据 D 提交运营平台。

[0023] 步骤 103：客户端 11 在服务器 12 执行步骤 102 的同时，开始对数据 D 进行签名处理。

[0024] 步骤 104：客户端 11 向服务器 12 发送数据签名 S 和数据 D。

[0025] 步骤 105：服务器 12 接收数据 D 和数据签名 S 后，对数据签名 S 进行验证，若通过执行步骤 106，否则执行步骤 107。

[0026] 步骤 106：服务器 12 不再进行任何处理，保持对数据 D 的提交状态。

[0027] 步骤 107：取消对数据的提交。

[0028] 其中步骤 101 中，用户甲需要通过客户端输入用于交易的数据 D，如以 5 元 / 股的价位，买入代码 12345 的股票 1000 股，或以 10 元 / 股的价位，卖出代码 54321 的股票 2000 股，输入完成后就可以通过客户端 11 向服务器 12 发送数据 D。

[0029] 其中步骤 102 中，服务器 12 接收数据 D 后，需确认数据 D 是否有效，如用户甲的付款帐户是否有 5000 元，用户甲的股票帐户是否有 2000 股代码 54321 的股票。确认数据 D 有效后将数据 D 提交股票交易运营平台。

[0030] 其中步骤 103 中，用户甲准备好用于交易的数据 D 后，根据预存在客户端 11 的私钥对数据 D 进行加密即进行签名处理，该过程是与步骤 102 服务器 12 接收数据 D，并确认数

据 D 是否有效的过程同步进行。

[0031] 其中步骤 104 中，在进行签名处理生成数据签名 S 后，客户端 11 将私钥签名后的数据 D 即数据签名 S 和数据 D 向服务器 12 发送，当然本步骤中也可以只发送数据签名 S，在后续步骤对数据签名 S 进行验证时采用步骤 101 中发送的数据 D。

[0032] 在步骤 104 和步骤 105 之间，还可以执行下述的步骤，服务器 12 判断是否在预定时间 T_A 内收到数据签名 S，若是则执行步骤 105，否则执行步骤 107，这样可以确保若客户端 11 和服务器 12 有传输时延或有故障重发时，通过设置的一个预定时间，以防止时延过长超出正常的数据 D 的有效性确认时间。

[0033] 其中步骤 105 中，服务器 12 根据公钥对数据签名 S 进行解密，将解密的结果和接收的数据 D 进行比较，若相同，则认为验证通过，否则，认为验证失败。

[0034] 其中步骤 106 中，服务器 12 不再进行任何处理，保持对数据 D 的提交状态。本步骤中并不马上通知客户端 11 数据 D 提交成功，而是要等到数据签名 S 被验证确认后才通知客户端 11 数据 D 提交成功。

[0035] 其中步骤 107 中，取消对数据的提交，具体实施时可以是向运营平台发送取消提交请求，并通知客户端 11 数据 D 提交失败，即向证交所提交撤单，并反馈用户订单失败。

[0036] 本发明第二实施例提供了一种数据签名验证的方法，本实施例以一个证券交易系统为例进行说明，该证券交易系统包括客户端 11 和服务器 12，客户端 11 和服务器 12 通过网络连接，该方法如图 2 所示，具体包括以下步骤：

[0037] 步骤 201：客户端 11 对数据 D 进行签名处理。

[0038] 步骤 202：客户端 11 向服务器 12 发送用于交易的数据 D 以及数据签名 S。

[0039] 步骤 203：服务器 12 接收数据 D，并确认数据 D 有效后将数据 D 提交运营平台。

[0040] 步骤 204：服务器 12 接收数据 D 和数据签名 S 后，在执行步骤 203 的同时，对数据签名 S 进行验证，若通过执行步骤 205，否则执行步骤 206。

[0041] 步骤 205：服务器 12 不再进行任何处理，保持对数据 D 的提交状态。

[0042] 步骤 206：取消对数据的提交。

[0043] 在第二实施例中，与第一实施例不同之处在于，服务器 12 是在确认数据 D 有效的同时，对数据签名 S 进行验证，而实施例一是服务器 12 确认数据 D 有效，与客户端 11 对数据 D 进行签名处理同步进行。

[0044] 通过上述的两个实施例可知，上述方案的关键是，服务器 12 接收客户端 11 发送的数据 D 并确认数据 D 是否有效的这一过程，和客户端 11 产生数据签名 S，服务器 12 对数据签名 S 进行验证这一过程同步进行，不论是实施例一的方案还是实施例二的方案，关键在于当数据签名 D 验证成功时，保持对没有经过签名验证就直接将数据 D 提交运营平台的提交状态，其中从时限上，数据签名 S 验证成功的时间，要晚于数据 D 提交运营平台的起始时间。

[0045] 下面对采用上述方案后所带来的有益效果进行说明，现有技术中，客户端 11 准备用于交易的数据 D 的时间为 T1，客户端 11 对数据 D 进行签名处理的时间为 T2，服务器 12 对数据签名 S 进行验证的时间为 T3，服务器 12 确认数据 D 有效的时间为 T4，这样从客户端 11 开始准备数据 D 到最终服务器 12 确认数据 D 有效，整个流程所需的时间为 T1+T2+T3+T4。若采用实施例 1 的方案，从客户端 11 开始准备数据 D 到最终服务器 12 确认数据 D 有效，整

个流程所需的时间为 T1+T4。若采用实施例 2 的方案，从客户端 11 开始准备数据 D 到最终服务器 12 确认数据 D 有效，整个流程所需的时间为 T1+T2+T4。当然，对于其它的方案，由于从时限上，数据签名 S 验证成功的时间即 T3 的结束时间点，要晚于对数据 D 提交运营平台的起始时间即 T4 的起始时间点。这样可以保证该方案整个流程的时间小于 T1+T2+T3+T4，使得基于数据签名验证过程数据安全性得到保证的前提下，减短了数据提交运营平台的时间。

[0046] 正是由于当数据签名验证成功的时间，晚于对数据提交运营平台的起始时间，确定对数据提交生效，使得基于数据签名验证过程数据安全性得到保证的前提下，减短了数据提交运营平台的时间。

[0047] 本发明第三实施例提供了一种数据签名验证的装置，如图 3 所示，包括：

[0048] 接收模块 301，用于接收客户端发送的数据和数据签名；

[0049] 数据确认模块 302，用于确认所述数据有效后将所述数据提交运营平台；

[0050] 数据验证模块 303，用于对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

[0051] 进一步，数据验证模块 303，还用于确认所述数据有效后，若预定时间内没有收到数据签名，则撤销所述数据的提交。

[0052] 进一步，数据确认模块 302，还用于在客户端对数据进行签名处理的同时，接收客户端发送的数据并确认数据有效，或者，客户端对数据进行签名处理后，接收客户端发送的数据，在对数据签名进行验证的同时，对数据的有效性进行确认。

[0053] 进一步，接收模块 301，还用于接收数据以及包含所述数据和数据签名的数据包。

[0054] 本发明第四实施例提供了一种数据签名验证的系统，如图 4 所示，包括：

[0055] 客户端 401，用于向服务器发送数据和数据签名；

[0056] 服务器 402，用于接收客户端发送的数据和数据签名，确认所述数据有效后将所述数据提交运营平台，对数据签名进行验证，若数据签名验证成功，则维持所述数据的提交状态，否则，撤销所述数据的提交。

[0057] 进一步，客户端 401，还用于向服务器发送数据以及包含所述数据和数据签名的数据包。

[0058] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0059] 本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

[0060] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

[0061] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

[0062] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

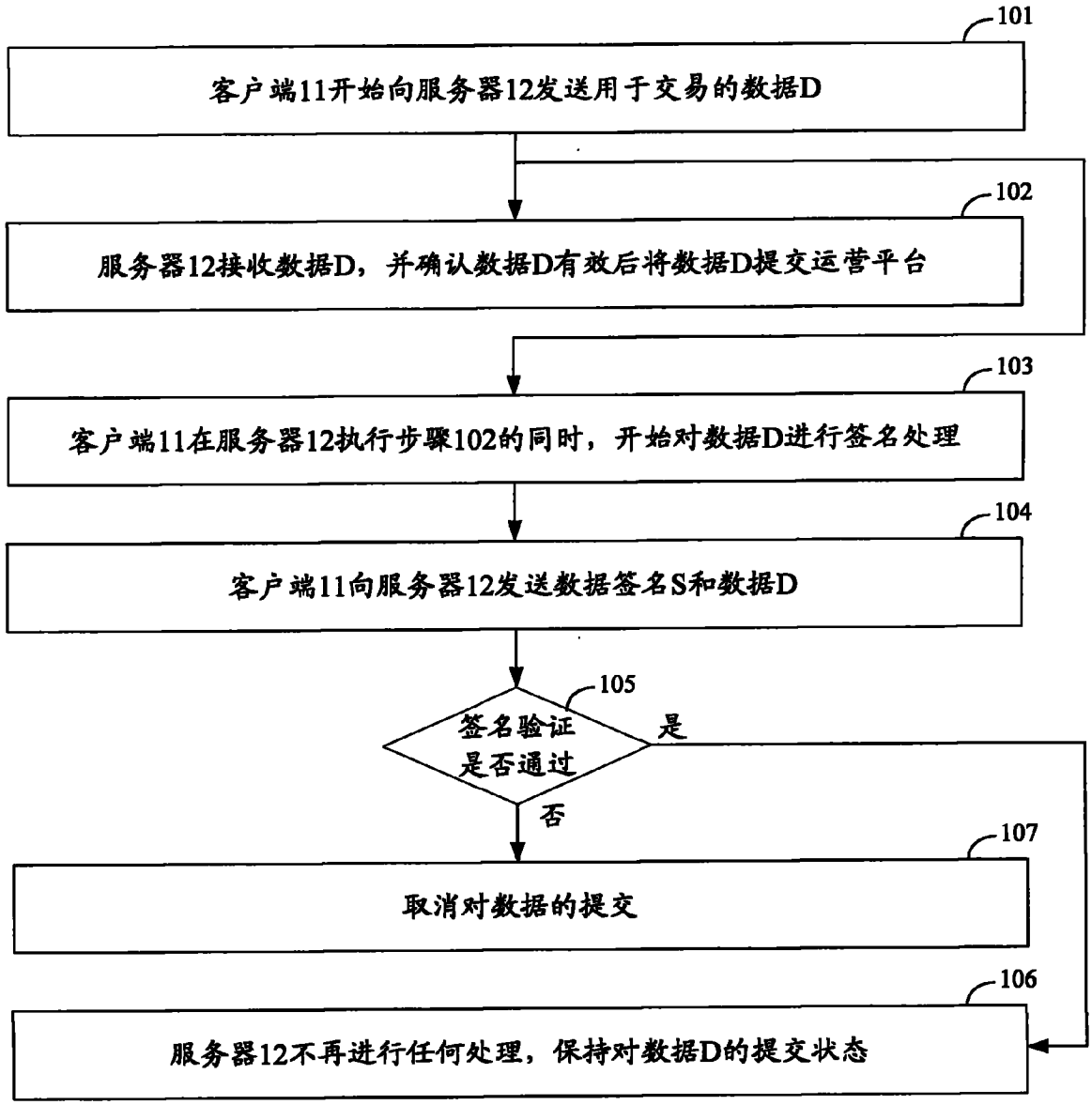

101
客户端11开始向服务器12发送用于交易的数据D
102
服务器12接收数据D，并确认数据D有效后将数据D提交运营平台
103
客户端11在服务器12执行步骤102的同时，开始对数据D进行签名处理
104
客户端11向服务器12发送数据签名S和数据D
105
签名验证是否通过
是
否
107
取消对数据的提交
106
服务器12不再进行任何处理，保持对数据D的提交状态

图 1

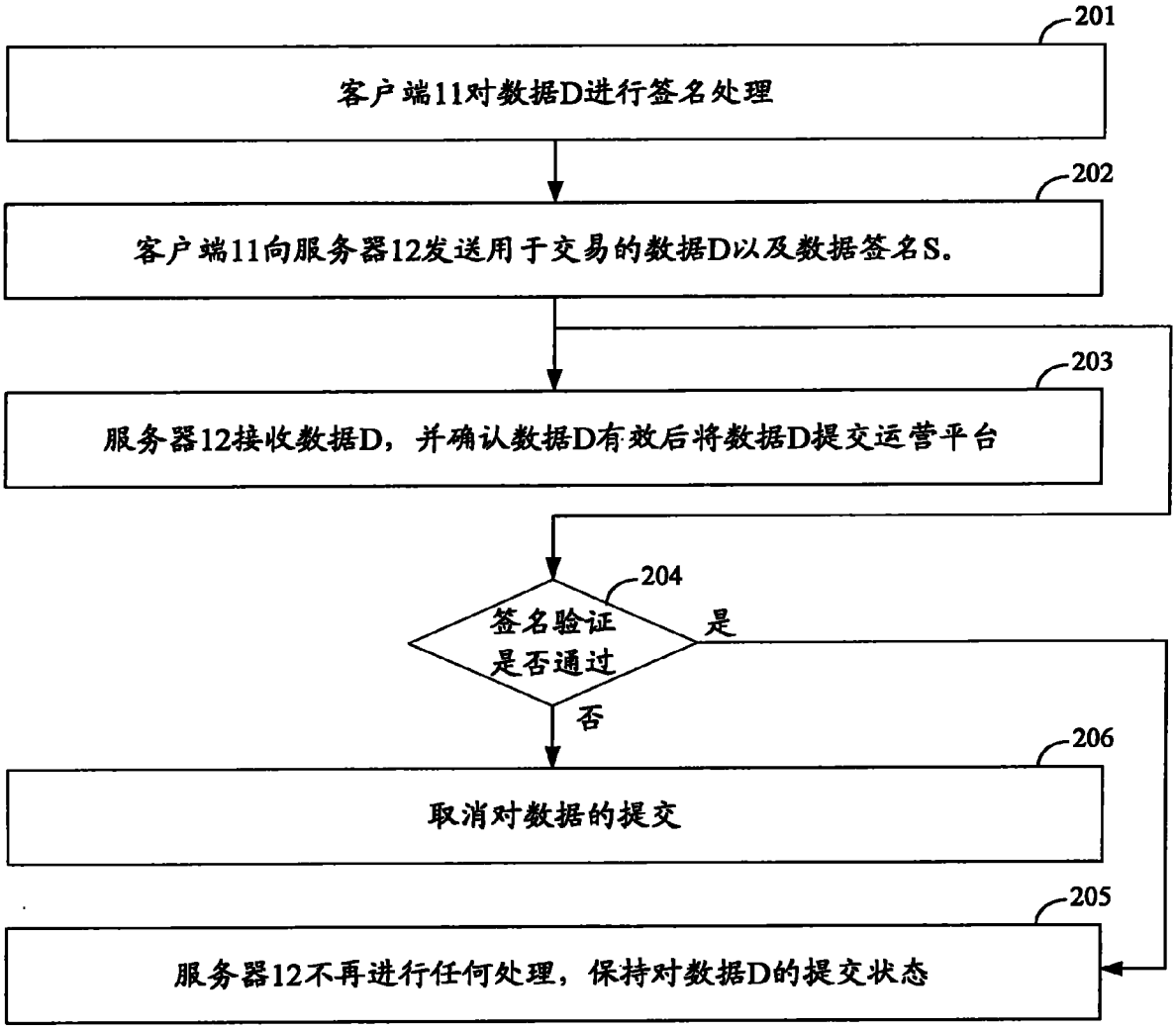

201
客户端11对数据D进行签名处理
202
客户端11向服务器12发送用于交易的数据D以及数据签名S。
203
服务器12接收数据D，并确认数据D有效后将数据D提交运营平台
204
签名验证是否通过
是
否
206
取消对数据的提交
205
服务器12不再进行任何处理，保持对数据D的提交状态

图 2

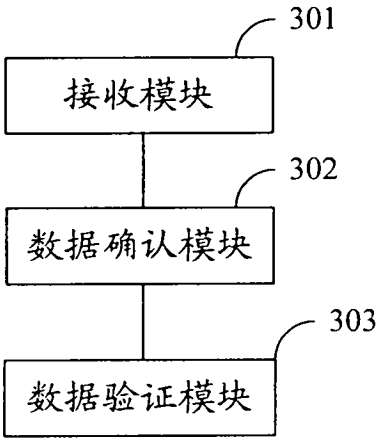

301
接收模块
302
数据确认模块
303
数据验证模块

图 3

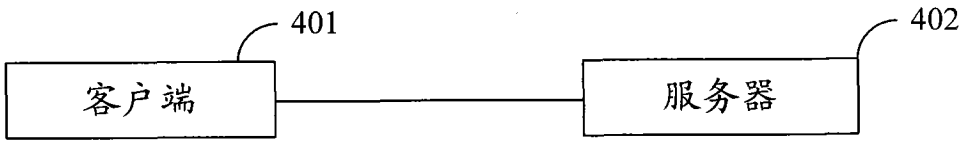


图 4