(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 112738117 A
(43)申请公布日 2021.04.30

(21)申请号 202011642016.4

(22)申请日 2020.12.31

(71)申请人 青岛海尔科技有限公司
地址 266101 山东省青岛市崂山区海尔路1号海尔工业园
申请人 海尔智家股份有限公司

(72)发明人 马俊岭

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 周婷婷

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

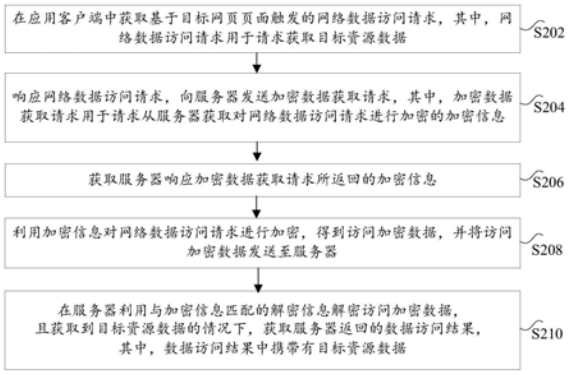
权利要求书3页 说明书15页 附图6页

(54)发明名称

数据传输方法、装置、系统和存储介质及电子装置

(57)摘要

本发明公开了一种数据传输方法、装置、系统和存储介质及电子装置。其中，该方法包括：在应用客户端中获取基于目标网页页面触发的网络数据访问请求，其中，网络数据访问请求用于请求获取目标资源数据；响应网络数据访问请求，向服务器发送加密数据获取请求；获取服务器响应加密数据获取请求所返回的加密信息；利用加密信息对网络数据访问请求进行加密，得到访问加密数据，并将访问加密数据发送至服务器；在服务器利用与加密信息匹配的解密访问加密数据，且获取到目标资源数据的情况下，获取服务器返回的数据访问结果。本发明解决了数据传输过程中安全性较低的技术问题。



CN 112738117 A

1.一种数据传输方法,应用于应用客户端,其特征在于,包括:

获取基于目标网页页面触发的网络数据访问请求,其中,所述网络数据访问请求用于请求获取目标资源数据;

响应所述网络数据访问请求,向服务器发送加密数据获取请求,其中,所述加密数据获取请求用于请求从所述服务器获取对所述网络数据访问请求进行加密的加密信息;

获取所述服务器响应所述加密数据获取请求所返回的所述加密信息;

利用所述加密信息对所述网络数据访问请求进行加密,得到访问加密数据,并将所述访问加密数据发送至所述服务器;

在所述服务器利用与所述加密信息匹配的解密信息解密所述访问加密数据,且获取到所述目标资源数据的情况下,获取所述服务器返回的数据访问结果,其中,所述数据访问结果中携带有所述目标资源数据。

2.根据权利要求1所述的方法,其特征在于,所述利用所述加密信息对所述网络数据访问请求进行加密,得到所述访问加密数据包括:

在所述加密信息包括加密方式和加密密钥的情况下,利用所述加密密钥按照所述加密方式对所述网络数据访问请求进行加密,并添加数字签名,以得到所述访问加密数据,其中,所述数字签名用于校验所述网络数据访问请求是否完整。

3.根据权利要求1所述的方法,其特征在于,所述获取所述服务器返回的数据访问结果包括:

获取所述服务器发送的利用所述加密信息对所述目标资源数据加密得到的所述数据访问结果;

利用与所述加密信息匹配的解密信息对所述数据访问结果进行解密,以获取所述目标资源数据,并将所述目标资源数据展示在所述目标网页页面中。

4.根据权利要求1所述的方法,其特征在于,在所述获取基于目标网页页面触发的网络数据访问请求之后,所述方法还包括:

生成所述应用客户端所在硬件设备的设备标识,其中,所述设备标识用于唯一标记所述硬件设备;

将所述设备标识存储至所述硬件设备的本地,并将所述设备标识添加至所述加密数据获取请求中。

5.一种数据传输方法,应用于服务器,其特征在于,包括:

在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下,接收所述应用客户端发送的加密数据获取请求,其中,所述网络数据访问请求用于请求访问目标资源数据,所述加密数据获取请求用于请求获取对所述网络数据访问请求进行加密的加密信息;

生成所述加密信息,并将所述加密信息发送至所述应用客户端,以使所述应用客户端利用所述加密信息对所述网络数据访问请求进行加密,得到访问加密数据;

接收所述应用客户端发送的所述访问加密数据;

在利用与所述加密信息匹配的解密信息解密所述访问加密数据的情况下,获取数据访问结果,并将所述数据访问结果发送给所述应用客户端,其中,所述数据访问结果中携带有所述目标资源数据。

6.根据权利要求5所述的方法,其特征在于,所述生成所述加密信息包括:

对所述加密数据获取请求进行身份验证；

在通过身份验证的情况下，获取当前所要使用的加密方式和加密密钥，以生成所述加密信息。

7.根据权利要求6所述的方法，其特征在于，所述对所述加密数据获取请求进行身份验证包括以下至少之一：

获取所述应用客户端对应的IP地址，并确定通过所述IP地址执行的网络数据访问行为的访问频次，其中，在所述访问频次小于第一阈值的情况下，确定所述IP地址通过IP访问验证，所述身份验证包括所述IP访问验证；

获取所述应用客户端所在硬件设备的设备标识，并确定通过所述硬件设备执行的网络数据访问行为的第一访问次数，其中，所述第一访问次数小于第二阈值的情况下，确定所述设备标识通过设备访问验证，所述身份验证包括所述设备访问验证；

获取所述应用客户端所使用的账号标识，并获取所述账号标识的身份信息，和通过所述账号标识执行的网络数据访问行为的第二访问次数，其中，所述第二访问次数小于第三阈值的情况下，确定所述账号标识通过账号访问验证，所述身份验证包括所述账号访问验证。

8.根据权利要求6所述的方法，其特征在于，在所述接收所述应用客户端发送的加密后的所述网络数据访问请求之后，还包括：

对所述加密信息中的所述加密密钥进行时效校验；

在所述加密密钥的使用时长已超出目标时间段的情况下，通知所述应用客户端所述网络数据访问请求已超时；

在所述加密密钥的使用时长并未超出所述目标时间段的情况下，使用本地生成的第一数字签名，对加密后的所述网络数据访问请求中携带的第二数字签名进行校验，其中，所述第二数字签名用于校验所述网络数据访问请求是否完整；

在所述第一数字签名与所述第二数字签名一致的情况下，确定所述网络数据访问请求未被修改，且成功解密所述网络数据访问请求。

9.根据权利要求6所述的方法，其特征在于，所述获取数据访问结果包括：

响应所述网络数据访问请求，获取所述目标资源数据；

利用所述加密信息对所述目标资源数据进行加密，得到所述数据访问结果。

10.根据权利要求5至9中任一项所述的方法，其特征在于：

所述加密信息中配置有目标时间段，在所述目标时间段的结束时刻时，删除本地存储的所述加密信息。

11.一种数据传输装置，应用于应用客户端，其特征在于，包括：

获取模块，用于获取基于目标网页页面触发的网络数据访问请求，其中所述网络数据访问请求用于请求获取目标资源数据；

第一发送模块，用于相应所述网络数据访问请求，向服务器发送加密数据获取请求，其中，所述加密数据获取请求用于请求从所述服务器获取对所述网络数据访问请求进行加密的加密信息；

第一接收模块，用于获取所述服务器响应所述加密数据获取请求所返回的所述加密信息；

加密模块，用于利用所述加密信息对所述网络数据访问请求进行加密，得到访问加密数据，并将所述访问加密数据发送至所述服务器；

第二接收模块，用于在所述服务器利用与所述加密信息匹配的解密信息解密所述访问加密数据，且获取到所述目标资源数据的情况下，获取所述服务器返回的数据访问结果，其中，所述数据访问结果中携带有所述目标资源数据。

12.一种数据传输装置，应用于服务器，其特征在于，包括：

第一接收模块，用于在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收所述应用客户端发送的加密数据获取请求，其中，所述网络数据访问请求用于请求获取目标资源数据，所述加密数据获取请求用于请求获取对所述网络数据访问请求进行加密的加密信息；

生成模块，用于生成所述加密信息，并将所述加密信息发送给所述应用客户端，以使所述应用客户端利用所述加密信息对所述网络数据访问请求进行加密，得到访问加密数据；

第二接收模块，用于接收所述应用客户端发送的所述访问加密数据；

处理模块，用于在利用与所述加密信息匹配的解密信息解密所述访问加密数据的情况下，获取数据访问结果，并将所述数据访问结果发送给所述应用客户端，其中，所述数据访问结果中携带有所述目标资源数据。

13.一种数据传输系统，其特征在于，包括：

应用客户端响应基于目标网页页面触发的网络数据访问请求，向服务器发送加密数据获取请求，其中，所述网络数据访问请求用于请求获取目标资源数据；

所述服务器响应所述加密数据获取请求，生成加密信息；

所述应用客户端根据所述加密信息对所述网络数据访问请求进行加密，并将生成的访问加密数据发送给所述服务器；

所述服务器处理所述访问加密数据，得到数据访问结果，并将所述数据访问结果发给所述应用客户端，其中，所述数据访问结果中携带有所述目标资源数据；

所述应用客户端接收所述数据访问结果。

14.一种计算机可读的存储介质，其特征在于，所述计算机可读的存储介质包括存储的程序，其中，所述程序运行时执行所述权利要求1至4任一项中所述的方法或权利要求5至10任一项中所述的方法。

15.一种电子装置，包括存储器和处理器，其特征在于，所述存储器中存储有计算机程序，所述处理器被设置为通过所述计算机程序执行所述权利要求1至4任一项中所述的方法或权利要求5至10任一项中所述的方法。

数据传输方法、装置、系统和存储介质及电子装置

技术领域

[0001] 本发明涉及应用数据传输领域，具体而言，涉及一种数据传输方法、装置、系统和存储介质及电子装置。

背景技术

[0002] 目前，很多应用客户端均可以通过发送链接的方式进行信息分享，分享的链接通常以网页的形式展现。而网页中通常包含有很多关键数据，例如抽奖页面中包含的个人信息、支付网页中所包含的支付信息。

[0003] 而未经加密的网页发起的数据请求，通过查看网页页面源码，即可获得其数据请求方式。再者，通过Http抓包就可以截获数据请求，从而模拟其数据请求的方式发起对服务器或应用客户端的攻击，因此需要对网页进行加密以保证数据传输的安全。但相关技术提供的数据传输方法往往是直接传输，使得数据传输过程中关键数据易丢失、易被篡改，从而导致数据传输安全性较低的问题。

[0004] 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

[0005] 本发明实施例提供了一种数据传输方法、装置、系统和存储介质及电子装置，以至少解决数据传输过程中安全性较低的技术问题。

[0006] 根据本发明实施例的一个方面，提供了一种数据传输方法，包括：在应用客户端中获取基于目标网页页面触发的网络数据访问请求，其中，上述网络数据访问请求用于请求获取目标资源数据；响应上述网络数据访问请求，向服务器发送加密数据获取请求，其中，上述加密数据获取请求用于请求从上述服务器获取对上述网络数据访问请求进行加密的加密信息；获取上述服务器响应上述加密数据获取请求所返回的上述加密信息；利用上述加密信息对上述网络数据访问请求进行加密，得到访问加密数据，并将上述访问加密数据发送至上述服务器；在上述服务器利用与上述加密信息匹配的解密信息解密上述访问加密数据，且获取到上述目标资源数据的情况下，获取上述服务器返回的数据访问结果，其中，上述数据访问结果中携带有上述目标资源数据。

[0007] 根据本发明实施例的一个方面，还提供了一种数据传输方法，包括：在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收上述应用客户端发送的加密数据获取请求，其中，上述网络数据访问请求用于请求获取目标资源数据，上述加密数据获取请求用于请求获取对上述网络数据访问请求进行加密的加密信息；生成上述加密信息，并将上述加密信息发送给上述应用客户端，以使上述应用客户端利用上述加密信息对上述网络数据访问请求进行加密，得到上述访问加密数据；接收上述应用客户端发送的上述访问加密数据；在利用与上述加密信息匹配的解密信息解密上述访问加密数据的情况下，获取数据访问结果，并将上述数据访问结果发送给上述应用客户端，其中，上述数据访问结果中携带有上述目标资源数据。

[0008] 根据本发明实施例的一个方面，还提供了一种数据传输装置，应用于应用客户端中，包括：获取模块，用于获取基于目标网页页面触发的网络数据访问请求，其中上述网络数据访问请求用于请求获取目标资源数据；第一发送模块，用于相应上述网络数据访问请求，向服务器发送加密数据获取请求，其中，上述加密数据获取请求用于请求从上述服务器获取对上述网络数据访问请求进行加密的加密信息；第一接收模块，用于获取上述服务器响应上述加密数据获取请求所返回的上述加密信息；加密模块，用于利用上述加密信息对上述网络数据访问请求进行加密，得到访问加密数据，并将上述访问加密数据发送至上述服务器；第二接收模块，用于在上述服务器利用与上述加密信息匹配的解密信息解密上述访问加密数据，且获取到上述目标资源数据的情况下，获取上述服务器返回的数据访问结果，其中，上述数据访问结果中携带有上述目标资源数据。

[0009] 根据本发明实施例的一个方面，还提供了一种数据传输装置，应用于应用服务器中，包括：第一接收模块，用于在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收上述应用客户端发送的加密数据获取请求，其中，上述网络数据访问请求用于请求获取目标资源数据，上述加密数据获取请求用于请求获取对上述网络数据访问请求进行加密的加密信息；生成模块，用于生成上述加密信息，并将上述加密信息发送给上述应用客户端，以使上述应用客户端利用上述加密信息对上述网络数据访问请求进行加密，得到访问加密数据；第二接收模块，用于接收上述应用客户端发送的上述访问加密数据；处理模块，用于在利用与上述加密信息匹配的解密信息解密上述访问加密数据的情况下，获取数据访问结果，并将上述数据访问结果发送给上述应用客户端，其中，上述数据访问结果中携带有上述目标资源数据。

[0010] 根据本发明实施例的一个方面，还提供了一种数据传输系统，包括：应用客户端响应基于目标网页页面触发的网络数据访问请求，向服务器发送加密数据获取请求，其中，上述网络数据访问请求用于请求获取目标资源数据；上述服务器响应上述加密数据获取请求，生成加密信息；上述应用客户端根据上述加密信息对上述网络数据访问请求进行加密，并将生成的访问加密数据发送给上述服务器；上述服务器处理上述访问加密数据，得到数据访问结果，并将上述数据访问结果发给上述应用客户端，其中，上述数据访问结果中携带有上述目标资源数据；上述应用客户端接收上述数据访问结果。

[0011] 根据本发明实施例的又一方面，还提供了一种计算机可读的存储介质，该计算机可读的存储介质中存储有计算机程序，其中，该计算机程序被设置为运行时执行上述数据传输方法。

[0012] 根据本发明实施例的又一方面，还提供了一种电子装置，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，上述处理器通过计算机程序执行上述的数据传输方法。

[0013] 在本发明实施例中，通过应用客户端基于目标页面触发的网络数据访问请求向服务器发起加密数据获取请求，在服务器对于加密数据获取请求验证通过后，应用客户端根据服务器返回的加密信息对网络数据访问请求进行加密，服务器验证加密数据获取请求后，将处理得到的数据访问结果基于同样的加密信息加密后发送应用客户端，实现了加密信息的动态获取，以及在网络数据访问请求发送和指示访问结果的目标资源数据发送的双向网络数据传输加密，达到了对目标页面发起的访问请求和接收的结果数据双向加密地安

全传输，从而实现了提高数据传输安全性的技术效果，解决了数据传输过程中安全性较低的技术问题。

附图说明

[0014] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0015] 图1是根据本发明实施例的一种可选的数据传输方法的应用环境的示意图；

[0016] 图2是根据本发明实施例的一种可选的数据传输方法的实施流程的示意图；

[0017] 图3是根据本发明实施例的一种可选的数据传输方法的实施流程的示意图；

[0018] 图4是根据本发明实施例的一种可选的数据传输方法的实施流程的示意图；

[0019] 图5是根据本发明实施例的一种可选的数据传输方法的实施流程的示意图；

[0020] 图6是根据本发明实施例的一种可选的数据传输方法的实施流程的示意图；

[0021] 图7是根据本发明实施例的一种可选的数据传输方法的交互时序示意图；

[0022] 图8是根据本发明实施例的一种可选的数据传输的界面交互示意图；

[0023] 图9是根据本发明实施例的一种可选的数据传输装置的结构示意图；

[0024] 图10是根据本发明实施例的一种可选的数据传输装置的结构示意图；

[0025] 图11是根据本发明实施例的一种可选的电子设备的结构示意图。

具体实施方式

[0026] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0027] 需要说明的是，本发明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，以便这里描述的本发明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。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0028] 根据本发明实施例的一个方面，提供了一种数据传输方法，可选地，作为一种可选的实施方式，上述数据传输方法可以但不限于应用于如图1所示的环境中。应用环境中包括用户设备102，安装在用户设备102上的应用客户端104、网络110以及服务器112。用户设备102和应用客户端104基于网络110与服务器112进行数据交互。

[0029] 可选地，在本实施例中，上述数据传输方法可以但不限于应用于应用客户端104中，用于协助应用客户端对目标页面进行数据传输处理。其中，上述应用客户端104可以但不限于运行在用户设备102中，该用户设备102可以但不限于为手机、平板电脑、笔记本电脑、PC机等支持运行应用客户端104的终端设备。服务器112和用户设备102可以但不限于通

过网络110实现数据交互，上述网络110可以包括但不限于无线网络或有线网络。其中，该无线网络包括：蓝牙、WIFI及其他实现无线通信的网络。上述有线网络可以包括但不限于：广域网、城域网、局域网。上述仅是一种示例，本实施例中对此不作任何限定。

[0030] 可选地，作为一种可选的实施方式，如图2所示，上述数据传输方法包括：

[0031] S202，在应用客户端中获取基于目标网页页面触发的网络数据访问请求，其中，网络数据访问请求用于请求获取目标资源数据；

[0032] S204，响应网络数据访问请求，向服务器发送加密数据获取请求，其中，加密数据获取请求用于请求从服务器获取对网络数据访问请求进行加密的加密信息；

[0033] S206，获取服务器响应加密数据获取请求所返回的加密信息；

[0034] S208，利用加密信息对网络数据访问请求进行加密，得到访问加密数据，并将访问加密数据发送至服务器；

[0035] S210，在服务器利用与加密信息匹配的解密信息解密访问加密数据，且获取到目标资源数据的情况下，获取服务器返回的数据访问结果，其中，数据访问结果中携带有目标资源数据。

[0036] 上述服务器是指与上述应用客户端对应的服务器，通过网络与应用客户端交互，处理应用客户端的数据请求。

[0037] 上述应用客户端是指安装在终端设备中、能够发起网络分享页面的客户端。上述目标页面是指由应用客户端发起的、需要进行网络数据处理的网络页面。可选地，目标页面中可以包括但不限于：文字、图片、视频、触发按键。触发按键可以但不限于：用于触发网络数据访问请求，以获取数据访问结果。目标页面可以但不限于是：抽奖页面、测试页面、确认页面。所对应的数据访问结果不限于是：获奖信息、测试结果、确认信息。上述目标资源数据是指对数据访问结果解密后得到的访问结果，通常以包含有关键信息的结果页面的形式呈现，关键信息可以不限于是：关键文字、关键图片。

[0038] 可选地，在本申请实施例中，上述目标网页可以但不限于是：H5页面。H5页面是指基于HTML5(第五代超文本标记语言)制作的页面，是可以承载文本、图片、音视频的流媒体格式、在移动终端展示的动态页面。

[0039] 可选地，在本申请实施例中，上述加密信息可以但不限于是服务器随机生成的，服务器根据加密数据获取请求的相关信息生成的，相关信息可以但不限于是：加密数据请求的类型，加密数据的类型。

[0040] 可选地，在本申请实施例中，上述加密信息可以包括但不限于以下至少之一：加密方式、加密密钥、加密算法。加密方式可以但不限于以下至少之一：DES、AES、blowfish。加密密钥可以但不限于是：动态密钥、对称密钥、非对称密钥。加密算法可以但不限于是：已有的加密算法、特制的加密算法。

[0041] 在本发明实施例中，通过应用客户端基于目标页面触发的网络数据访问请求向服务器发起加密数据获取请求，在服务器对于加密数据获取请求验证通过后，应用客户端根据服务器返回的加密信息对网络数据访问请求进行加密，服务器验证加密数据获取请求后，将处理得到的目标资源数据基于同样的加密信息加密生成数据访问结果发送应用客户端，实现了加密信息的动态获取，以及在网络数据访问请求发送和目标资源数据发送的双向网络数据传输加密，达到了对目标页面发起的网络数据访问请求和接收的目标资源数据

双向加密地安全传输，从而实现了提高数据传输安全性的技术效果，解决了数据传输过程中安全性较低的技术问题。

[0042] 作为一种可选的实施方式，上述利用加密信息对网络数据访问请求进行加密，得到访问加密数据包括：

[0043] 在加密信息包括加密方式和加密密钥的情况下，利用加密密钥按照加密方式对网络数据访问请求进行加密，并添加数字签名，以得到访问加密数据，其中，数字签名用于校验网络数据访问请求是否完整。

[0044] 上述数字签名是对网络数据访问请求基于一定的算法运算后，添加在访问加密数据中，用于校验网络数据访问请求完整性的验证数据。可选地，数字签名采用的运算规则可以但不限于是：RSA、SHA。

[0045] 在本申请实施例中，加密信息是服务器根据应用客户端发送的加密数据获取请求动态生成的，在对网络数据访问请求加密的基础上，增加数字签名用于校验网络数据访问请求的完整性，进一步保证网络数据访问请求的传输安全性，避免网络数据访问请求被恶意访问和篡改。

[0046] 作为一种可选的实施方式，上述获取服务器返回的数据访问结果包括：

[0047] 获取服务器发送的利用加密信息加密对目标资源数据加密得到的数据访问结果；

[0048] 利用与加密信息匹配的解密信息对数据访问结果进行解密，以获取目标资源数据，并将目标资源数据展示在目标网页页面中。

[0049] 上述解密信息是与加密信息对应的解密方式、解密密钥、解密算法，是与加密信息对应的逻辑运算法则。解密信息与加密信息唯一对应。根据解密信息可以对应破解数据访问结果，以得到目标资源数据，从而展示在目标网页页面中。

[0050] 在本申请实施例中，数据访问结果是服务器在处理网络数据访问请求后对得到的目标资源数据根据加密信息加密后得到的，从而保证目标资源数据在传输过程中的安全性，避免了目标资源数据在传输过程中被恶意截获、访问和篡改。同时利用同样的加密信息对目标资源数据进行加密，减少了服务器再次生成加密方式和与应用客户端再次交互加密方式而给服务器带来的负荷以及数据传输所需的时间，利用同样的动态加密方式，在保证数据传输安全性的同时，也节省了数据传输所需耗费的时间。

[0051] 作为一种可选的实施方式，在上述获取基于目标网页页面触发的网络数据访问请求之后，方法还包括：

[0052] 生成应用客户端所在硬件设备的设备标识，其中，设备标识用于唯一标记硬件设备；

[0053] 将设备标识存储至硬件设备的本地，并将设备标识添加至加密数据获取请求中。

[0054] 设备标识是应用客户端用于表示自身所在终端的标识，用于区别多个应用客户端在于服务器交互过程中，服务器对于应用客户端的识别。

[0055] 可选地，设备标识可以但不限于是：应用客户端在终端中首次启动时基于终端相关信息随机生成的标识、应用客户端基于终端相关信息按照既定算法生成的标识。上述终端相关信息可以但不限于包括以下至少之一：终端序列号、终端地址、终端型号、终端ID。

[0056] 可选地，设备标识的生成规则可以但不限于：采用MD5运算规则。

[0057] 在本申请实施例中，应用客户端通过生成设备标识，用于表示自身所在终端的信

息，在与服务器交互的过程中，可以基于设备标识对终端进行识别，从而避免所在终端对网络数据进行恶意访问，从而保证网络数据传输的安全性。

[0058] 可选地，上述将设备标识存储至硬件设备的本地包括以下至少之一：

[0059] 将设备标识存储至硬件设备的本地系统文件存储空间中；

[0060] 将设备标识以隐藏文件形式存储至硬件设备的本地中。

[0061] 可选地，在上述两个存储空间中都存储有设备标识的情况下，优先从本地系统文件中读取。将设备标识存在的硬件设备的本地空间中，避免了设备标识被误删除，导致设备标识丢失的情况出现，保证了设备标识的唯一性。

[0062] 在本申请实施例中，设备标识用于标记应用客户端所在的硬件设备，设备标识能够便于服务器能够在中多个交互的应用客户端和硬件设备中进行快速识别。同时可以避免因没有设备标识造成的多次重复交互以及多次重复交互结果不同的情况出现，减轻服务器的处理负荷，保证了数据访问结果的唯一性。

[0063] 可选地，加密信息中配置有目标时间段，在目标时间段的结束时刻时，加密信息将从服务器中删除。

[0064] 上述目标时间段是服务器在生成加密信息时为加密密钥设置的有效时限，在目标时间段内，加密信息有效，目标时间段结束，加密信息则变更为无效状态。目标时间段相当于此加密密钥为网络数据访问请求开放的窗口期，在目标时间段内，网络数据访问请求能够被服务器接收、处理，超出目标时间段，加密密钥时效，访问请求过期。

[0065] 在本申请实施例中，服务器将在目标时间段结束时刻就被从服务器中删除，既避免了无用的加密信息占用服务器内存空间，同时还能够避免能够从服务器中获取加密信息从而发起恶意访问或数据截取，进一步保证了目标网页数据传输的安全性。

[0066] 根据本发明实施例的一个方面，提供了一种数据传输方法，如图3所示，包括：

[0067] S302，在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收应用客户端发送的加密数据获取请求，其中，网络数据访问请求用于请求获取目标资源数据，加密数据获取请求用于请求获取对网络数据访问请求进行加密的加密信息；

[0068] S304，生成加密信息，并将加密信息发送给应用客户端，以使应用客户端利用加密信息对网络数据访问请求进行加密，得到访问加密数据；

[0069] S306，接收应用客户端发送的访问加密数据；

[0070] S308，在利用与加密信息匹配的解密信息解密访问加密数据的情况下，获取数据访问结果，并将数据访问结果发送给应用客户端，其中，数据访问结果中携带有目标资源数据。

[0071] 在本申请实施例中，服务器根据加密数据获取请求生成加密信息，以使应用客户端根据加密信息对网络数据访问请求进行加密，对加密后的网络数据访问请求进行处理得到数据访问结果，再将数据访问返回结果返回给应用客户端，实现了对于目标页面的数据传输加密，使得目标页面的数据传输安全性更高，避免了目标网页数据传输方式被恶意获取从而造成的关键数据丢失或篡改。

[0072] 作为一种可选的实施方式，生成加密信息包括：

[0073] 对加密数据获取请求进行身份验证；

[0074] 在通过身份验证的情况下，获取当前所要使用的加密方式和加密密钥，以生成加

密信息。

[0075] 可选地，如图4所示，服务器执行步骤S402对加密数据获取请求进行身份验证，在身份验证通过的情况下，执行步骤S404获取当前所要使用的加密方式和加密密钥，生成加密信息。在身份验证不通过的情况下，执行步骤S406，通知应用客户端身份验证不通过。

[0076] 作为一种可选的实施方式，对加密数据获取请求进行身份验证包括以下至少之一：

[0077] 获取应用客户端对应的IP地址，并确定通过IP地址执行的网络数据访问行为的访问频次，其中，在访问频次小于第一阈值的情况下，确定IP地址通过IP访问验证，身份验证包括IP访问验证；

[0078] 获取应用客户端所在硬件设备的设备标识，并确定通过硬件设备执行的网络数据访问行为的第一访问次数，其中，第一访问次数小于第二阈值的情况下，确定设备标识通过设备访问验证，身份验证包括设备访问验证；

[0079] 获取应用客户端所使用的账号标识，并获取账号标识的身份信息，和通过账号标识执行的网络数据访问行为的第二访问次数，其中，第二访问次数小于第三阈值的情况下，确定账号标识通过账号访问验证，身份验证包括账号访问验证。

[0080] 可选地，在上述身份验证方式运用不止一种时，则服务器按照IP访问验证、设备访问验证、账号访问验证的顺序依次进行，在所设置的访问验证方式全部验证通过的情况下，才代表访问验证通过，任何一项访问验证不通过均视为访问验证不通过。如图5所示，以使用三种验证方式为例。服务器接收到加密数据获取请求时，首先执行步骤S502判断IP访问频次是否小于第一阈值，通过获取应用客户端对应的IP地址，确定IP地址发起网络数据访问请求的访问频次，若访问频次小于第一阈值，则执行步骤S504判断第一访问次数是否小于第二阈值，根据应用客户端所在硬件设备的设备标识，确定该硬件设备执行网络数据访问行为的第一访问次数，若第一访问次数小于第二阈值，则执行步骤S506判断第二访问次数是否小于第三阈值，根据应用客户端使用的账号标识，确定通过该账号执行的网络数据访问行为的第二访问次数，若第二访问次数小于第三阈值，则执行步骤S508判定身份验证通过。在步骤S502、S504、S508任意一项验证结果为否时，则执行步骤S510判定身份验证不通过。

[0081] 具体地，上述第一阈值、第二阈值、第三阈值可以根据实际网络数据访问请求的内容进行具体限定。可选地，第一阈值≥第二阈值≥第三阈值。

[0082] 在本申请实施例中，服务器对发起加密数据获取请求的应用客户端进行身份验证，对应用客户端对应的IP地址进行IP访问验证，对于同一IP的访问次数进行限制，限制使用同一IP地址的终端的访问次数，避免同一IP地址多次发起访问，从而拦截有可能发起恶意访问的IP地址。对应用客户端所在硬件设备的设备标识进行设备访问验证，限制同一硬件设备对于目标页面的访问次数，避免同一硬件设备使用不同IP地址发起多次访问，从而拦截有可能发起恶意访问的硬件设备。对应用客户端所使用的账号标识进行账号访问验证，避免同一账号通过不同应用客户端、IP地址进行多次访问，从而拦截有可能发起恶意访问的账号。通过对IP访问、设备访问和账号访问其中至少一种形式进行身份验证，避免了通过同一IP、硬件设备、用户账号发起超次访问，从而通过访问次数的限制避免恶意访问的发生，从而降低对网络数据恶意访问成功的可能性，达到提高网络数据传输的安全性的效果。

[0083] 作为一种可选的实施方式，在接收应用客户端发送的加密后的网络数据访问请求之后，还包括：

[0084] 对加密信息中的加密密钥进行时效校验；

[0085] 在加密密钥的使用时长已超出目标时间段的情况下，通知应用客户端网络数据访问请求已超时；

[0086] 在加密密钥的使用时长并未超出目标时间段的情况下，使用本地生成的第一数字签名，对加密后的网络数据访问请求中携带的第二数字签名进行校验，其中，第二数字签名用于校验网络数据访问请求是否完整；

[0087] 在第一数字签名与第二数字签名一致的情况下，确定网络数据访问请求未被修改，且成功解密网络数据访问请求。

[0088] 可选地，如图6所示，服务器在接收应用客户端发送的加密后的网络数据访问请求之后，执行步骤S602判断加密密钥是否在目标时间段内，通过加密后的网络数据访问请求中获取加密密钥，加密密钥在目标时间段内则证明加密密钥有效。在加密密钥在有效时间段内的情况下，执行步骤S604校验网络数据访问请求是否完整。具体地，服务器根据网络数据访问请求中携带的签名方式和网络数据访问请求，生成的第一数字签名，与网络数据访问请求中携带的第二数字签名进行比对，在第一数字签名与第二数字签名一致的情况下，判断网络数据访问请求完整，执行步骤S606解密网络数据访问请求。具体地，根据加密信息对应的解密信息对加密的网络数据访问请求进行解密，得到网络数据访问请求，从而使服务器能够对网络数据访问请求进行处理以得到目标资源数据。若加密密钥判断不在目标时间段内，则执行步骤S608通知应用客户端访问请求已超时。若校验网络数据访问请求并不完整，则执行步骤S610通知应用客户端网络数据访问请求不完整。

[0089] 可选地，在应用客户端收到访问请求已超时时，应用客户端可以重新基于网络数据访问请求发起加密数据获取请求以获取新的加密数据。在客户端收到网络数据访问请求不完整时，且加密密钥依旧处于目标时间段的情况下，重新对网络数据访问请求进行加密，并重新添加数据签名，进行再次传输。

[0090] 在本申请实施例中，通过对加密密钥添加时效，限制网络数据访问请求的有效窗口时间段。加密密钥在目标时间段内，代表网络数据访问能够被服务器接收并处理，从而得到目标资源数据。加密密钥不在目标时间段内，则代表网络数据访问已超时，服务器不再处理网络数据访问，并通知应用客户端以访问已超时。同时在加密密钥保障数据传输安全的情况下，添加数字签名以保证网络数据访问请求的数据完整性，避免网络数据访问请求在传输过程中被篡改。加密密钥和数字签名的双重验证，进一步提高数据传输的安全性。

[0091] 作为一种可选的实施方式，获取数据访问结果包括：

[0092] 响应网络数据访问请求，获取目标资源数据；

[0093] 利用加密信息对目标资源数据进行加密，得到数据访问结果。

[0094] 作为一种可选的实施方式，加密信息中配置有目标时间段，在目标时间段的结束时刻时，删除本地存储的加密信息。

[0095] 可选地，目标时间段的结束时刻可以但不限于是在将数据访问结果发送给应用客户端端的时刻，数据访问结果发送之后的某一时刻。

[0096] 在本申请实施例中，服务器根据加密信息对目标资源数据进行加密得到数据访问

结果，将数据访问结果发给应用客户端，避免了目标资源数据在传输过程中的被恶意访问、截取和篡改，同时，减少了应用客户端对于目标资源数据的加密方式再次获取，减少了交互次数，从而减轻服务器的负荷。

[0097] 具体地，加密信息对应的加密规则可以但不限于是：

[0098] 算法1(去空格(请求体)，密钥)；

[0099] 其中，算法1代表加密所采用的具体的算法名称，请求体是指请求数据，去空格(请求体)是指对请求数据执行去空格函数，“，密钥”是在去空格函数得到的数据后添加密钥，并用“，”分隔，最后对于(去空格(请求体)，密钥)经过算法1的运算得到加密后的请求数据。

[0100] 算法2(算法1(去空格(请求体)，密钥)，密钥)；

[0101] 其中，算法2代表加密所采用的具体的算法名称，是在算法1运算得到的结果数据后添加“，密钥”，并对得到的数据运用算法2再次进行算法加密。即利用两种算法对于请求数据进行两次加密，增加加密后的请求数据的破解难度，通过算法叠加进一步保证请求数据的安全性。

[0102] 可选地，数字签名的生成规则可以但不限于是：

[0103] SHA256(请求url+去空格(请求体)+appID+appKey+timestamp+密钥)；

[0104] SHA256是具体的算法规则名称，即利用SHA256算法生成数字签名。“请求url”代表数据的类型标识，去空格(请求体)是指对请求数据执行去空格函数，“appID”代表应用客户端的ID序列号，“appKey”代表应用客户端的接口验证序号，“timestamp”代表时间戳，“密钥”是加密数据中包含的加密密钥，上述六个数据分别用“+”连接构成一组数据，并利用SHA256算法进行运算后就可以得相应的数字签名。

[0105] 可选地，设备标识的生成规则可以但不限于是：

[0106] md5(sn+安装id+imei+mac+型号+androidid)；

[0107] md5是指运用的具体的算法的名称，“sn”是指硬件设备的产品序列号；“安装id”是指硬件设备的硬件标识与应用客户端id建立的安装id；“imei”是指硬件设备的硬件标识，“mac”是指硬件设备的通讯地址，“型号”是指硬件设备对应的型号标识；“androidid”是指硬件设备的系统类型，上述六个数据均采用“+”连接构成一组数据，经过md5算法运算即可得到设备标识。

[0108] 具体地，上述数据传输的实施方法可以但不限于如图7所示：

[0109] 目标页面701执行步骤S702，发起网络数据访问请求，用于请求访问目标资源数据，应用客户端703接收网络数据访问请求，执行步骤S704，生成设备标识。应用客户端703将设备标识存储在硬件设备的本地系统Settings文件中，可选地，备份在硬件设备的本地中，避免设备标识被误删。应用客户端703执行步骤S706，发起加密数据获取请求，并将设备标识添加在加密数据获取请求中。服务器705接收加密数据获取请求，并对加密数据获取请求进行身份验证。

[0110] 服务器705执行步骤S7082，IP访问验证。获取应用客户端所对应的IP地址，确定该IP地址在单位时间内对于网络数据访问的频次，如果单位时间内访问频次小于第一阈值，假设，单位时间设定为一秒钟，第一阈值设定为十次，则代表使用该IP在一秒钟内只能访问十次，如果此次访问行为是该IP第八次发起访问，则IP地址通过IP访问验证，如果此次访问形式是该IP第十一次发起访问，则IP地址不能通过IP访问验证，服务器705拒接应用客户端

703的加密数据获取请求，并通知应用客户端703。

[0111] 服务器705执行步骤S7084设备访问验证。获取加密数据请求中的设备标识，确定发起网络数据访问的硬件设备的第一访问次数，如果当前第一访问次数小于第二阈值，例如，第二阈值设定为五次，此次第一访问次数为第三次，则设备访问验证通过；如果此次第一访问次数为第五次，则设备访问验证不通过，服务器705拒绝应用客户端703的加密数据获取请求，并通知应用客户端703。

[0112] 服务器执行步骤S7086账号访问验证。获取账号标识的身份信息，确定账号执行网络数据访问行为的第二访问次数，如果当前的第二访问次数小于第三阈值，例如，第三阈值设定为三次，此次第二访问次数为第二次，则账号访问验证通过；如果此次第二访问次数为第三次，则账号访问验证不通过，服务器705拒绝应用客户端703的加密数据获取请求，并通知应用客户端703。

[0113] 在服务器705对加密数据获取请求的身份验证通过的情况下，执行步骤S7102生成加密信息。加密信息包括加密方式和加密密钥。

[0114] 服务器S7102在生成加密密钥后执行步骤S7104为加密密钥配置目标时间段，目标时间段即为加密密钥的有效期限，例如，十秒，在十秒内加密密钥为有效的密钥，超过十秒则加密密钥失效。由此避免了通过加密密钥恶意访问和获取网络数据。在完成为密钥配置目标时间段的情况下，服务器705执行步骤S712发送加密信息。

[0115] 应用客户端703在接收到服务器705发送的加密信息后，根据加密信息执行步骤S714加密网络数据访问请求，利用加密方式和加密密钥生成加密后的网络数据访问请求。然后，执行步骤S716发送加密的网络数据访问请求。

[0116] 服务器705在收到应用客户端703发送的加密的网络数据访问请求后，执行步骤S7182校验加密密钥时效，验证密钥是否在目标时间段内，假设目标时间段是十秒，如果密钥的使用时长未超出十秒，则密钥时效校验通过，如果密钥的使用时长超出十秒，则代表密钥已经失效，服务器705通知应用客户端访问请求已超时，同时拒绝对网络数据访问请求的处理。在密钥时效校验有效的情况下，服务器705执行步骤S7184校验数据完整性，数据完整性的校验是对数据访问请求中携带的数字签名进行校验。具体地，服务器705在本地通过数字签名的运算法则对网络数据访问请求进行运算，生成第一数字签名，对访问请求中携带的第二数字签名进行校验，在第一数字签名和第二数字签名一致的情况下，认为网络数据访问请求完整，在在网络数据访问请求校验结果为完整的情况下，服务器705处理网络数据访问请求，得到目标资源数据，将得到的目标资源数据根据加密信息进行加密，得到数据访问结果，之后执行步骤S720发送数据访问结果。

[0117] 应用客户端703在接收到服务器705发送的数据访问结果后，根据加密信息对应的解密信息执行步骤S722，解密数据访问结果，得到目标资源数据。应用客户端703执行步骤S724，发送目标资源数据，目标页面701在接收到目标资源数据后，将目标资源数据在页面中展示，由此，完成了目标页面701获取目标资源数据的目的。

[0118] 以目标页面为抽奖页面，目标资源数据为包含有抽奖结果的数据为例，进行本申请实施例的示例说明。如图8所示，当前为手机上运行“海尔之家”APP，并已经点击进入抽奖页面的画面。在手机终端802的屏幕上运行有海尔之家804的运行界面，此时海尔之家804的运行界面中显示有抽奖页面806，抽奖页面806中包含有用于奖品展示的展示区以及用于触

发抽奖指令的抽奖键808。用户点击抽奖键808，即触发了网络数据访问请求，本示例中为抽奖请求，用于请求目标资源数据即本示例中的抽奖结果。

[0119] 抽奖页面806将抽奖请求发送给海尔之家804，海尔之家804根据设备标识的生成规则：md5(sn+安装id+imei+mac+型号+androidid)，生成与当前手机和海尔之家804APP唯一对应的设备标识，并将设备标识保存在海尔之家804的系统Setting文件和手机终端802的存储空间内。海尔之家804执行步骤S801，发送加密数据获取请求，并将设备标识添加在加密数据获取请求中，服务器810收到加密数据获取请求后，首先进行身份验证。服务器810首先确定手机终端802所使用的IP地址、获取请求中包含的设备标识以及登录海尔之家804的用户账号。在本示例的抽奖活动中，设定第一阈值为5，第二阈值为2，第三阈值为2。假设本次是用户账号第1次使用手机终端802通过家庭网络发起的第1次抽奖请求，而之前已经有两位家庭成员分别使用各自的手机通过该家庭网络、分别发起过1次抽奖请求。即本次IP访问频次为3，第一访问次数为1，第二访问次数为1。服务器810首先判断IP访问频次小于第一阈值，然后判断第一访问次数小于第二阈值，最后判断第二访问次数小于第三阈值，由此判定身份验证通过。然后服务器810生成加密信息，加密信息包括加密算法和加密密钥，本示例中的加密密钥为公钥，加密算法是：DES(AES(去空格(请求体)，公钥)，公钥)，并未公钥配置目标时间段：十秒。然后服务器810执行步骤S803，发送加密信息给海尔之家804。

[0120] 海尔之家804根据接收的加密算法和公钥对抽奖请求进行加密，并根据数字签名规则：SHA256(请求url+去空格(请求体)+appID+appKey+timestamp+公钥)，生成第二数字签名，添加在加密后的抽奖请求中。然后，海尔之家804执行步骤S805发送加密后的抽奖请求。

[0121] 服务器810在收到加密后的抽奖请求时，首先判断公钥是否在十秒内，假设，本次服务器810在一秒后收到了加密的抽奖请求，即公钥有效。接下来，服务器810根据加密算法和公钥对加密的抽奖请求进行解密，得到抽奖请求，并根据数字签名规则计算生成第一数字签名，在第一数字签名与第二数据签名一致的情况下，认为抽奖请求的数据完整，并处理该抽奖请求，得到包含有“奖品二”的目标资源数据。服务器810根据加密算法和公钥对目标资源数据加密得到抽奖结果，并执行步骤S807，发送抽奖结果。

[0122] 海尔之家804接收到抽奖结果后，根据加密算法和公钥对抽奖结果进行解密，得到包含有“奖品二”的目标资源数据，并将其展示在抽奖页面812的结果显示区814上。如图8所示，抽奖页面812的结果显示区814上显示有“奖品二”。

[0123] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0124] 根据本发明实施例的又一个方面，还提供了一种数据传输装置，应用于应用客户端中，如图9所示，包括：

[0125] 获取模块902，用于获取基于目标网页页面触发的网络数据访问请求，其中网络数据访问请求用于请求访问目标资源数据；

[0126] 第一发送模块904，用于相应网络数据访问请求，向服务器发送加密数据获取请

求，其中，加密数据获取请求用于请求从服务器获取对网络数据访问请求进行加密的加密信息；

[0127] 第一接收模块906，用于获取服务器响应加密数据获取请求所返回的加密信息；

[0128] 加密模块908，用于利用加密信息对网络数据访问请求进行加密，得到加密后的网络数据访问请求，并将加密后的网络数据访问请求发送至服务器；

[0129] 第二接收模块910，用于在服务器利用与加密信息匹配的解密信息解密网络数据访问请求，且获取到目标资源数据的情况下，获取服务器返回的数据访问结果，其中，数据访问结果中携带有目标资源数据。

[0130] 在本申请实施例中，通过应用客户端获取模块获取到的基于目标页面触发的网络数据访问请求，通过第一发送模块向服务器发起加密数据获取请求，在服务器对于加密数据获取请求验证通过后，应用客户端通过第一接收模块接收服务器返回的加密信息，并通过加密模块对网络数据访问请求进行加密，服务器验证加密数据获取请求后，通过第二接收模块得到数据访问结果，并基于同样的加密信息加密后发送应用客户端，实现了加密信息的动态获取，以及在网络数据访问请求发送和数据访问结果发送的双向网络数据传输加密，达到了对目标页面发起的网络数据访问请求和接收的数据访问结果双向加密地安全传输，从而实现了提高数据传输安全性的技术效果，解决了数据传输过程中安全性较低的技术问题。

[0131] 根据本发明实施例的又一个方面，还提供了一种数据传输装置，应用于服务器中，如图10所示，包括：

[0132] 第一接收模块1002，用于在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收应用客户端发送的加密数据获取请求，其中，网络数据访问请求用于请求访问目标资源数据，加密数据获取请求用于请求获取对网络数据访问请求进行加密的加密信息；

[0133] 生成模块1004，用于生成加密信息，并将加密信息发送给应用客户端，以使应用客户端利用加密信息对网络数据访问请求进行加密，得到加密后的网络数据访问请求；

[0134] 第二接收模块1006，用于接收应用客户端发送的加密后的网络数据访问请求；

[0135] 处理模块1008，用于在利用与加密信息匹配的解密信息解密网络数据访问请求的情况下，获取数据访问结果，并将数据访问结果发送给应用客户端，其中，数据访问结果中携带有目标资源数据。

[0136] 在本申请实施例中，通过第一接收模块接收应用客户端基于目标页面触发的网络数据访问请求向服务器发起加密数据获取请求，服务器对于加密数据获取请求验证通过后，生成加密信息并将加密信息发送给应用客户端，第二接收模块接收服务器根据加密信息加密后的网络数据访问请求，服务器并通过处理模块对验证数据有效性并处理访问请求，再将加密得到的数据访问结果发给应用客户端，实现了加密信息的动态生成，以及在网络数据访问请求发送和数据访问结果发送的双向网络数据传输加密，达到了对目标页面发起的网络数据访问请求和接收的数据访问结果双向加密地安全传输，从而实现了提高数据传输安全性的技术效果，解决了数据传输过程中安全性较低的技术问题。

[0137] 根据本发明实施例的又一个方面，提供了一种数据传输系统，包括：

[0138] 应用客户端响应基于目标网页页面触发的网络数据访问请求，向服务器发送加密

数据获取请求，其中，网络数据访问请求用于请求访问目标资源数据；

[0139] 服务器响应加密数据获取请求，生成加密信息；

[0140] 应用客户端根据加密信息对网络数据访问请求进行加密，并将加密后的网络数据访问请求发送给服务器；

[0141] 服务器处理网络数据访问请求，得到数据访问结果，并将根据加密信息加密后的数据访问结果发给应用客户端，其中，数据访问结果中携带有目标资源数据；

[0142] 应用客户端接收数据访问结果。

[0143] 在本发明实施例中，通过应用客户端基于目标页面触发的网络数据访问请求向服务器发起加密数据获取请求，在服务器对于加密数据获取请求验证通过后，应用客户端根据服务器返回的加密信息对网络数据访问请求进行加密，服务器验证加密数据获取请求后，将处理得到的数据访问结果基于同样的加密信息加密后发送应用客户端，实现了加密信息的动态获取，以及在网络数据访问请求发送和数据访问结果发送的双向网络数据传输加密，达到了对目标页面发起的网络数据访问请求和接收的数据访问结果双向加密地安全传输，从而实现了提高数据传输安全性的技术效果，解决了数据传输过程中安全性较低的技术问题。

[0144] 根据本发明实施例的又一个方面，还提供了一种用于实施上述数据传输方法的电子装置，如图11所示，该电子装置包括存储器1102和处理器1104，该存储器1102中存储有计算机程序，该处理器1104被设置为通过计算机程序执行上述任一项方法实施例中的步骤。

[0145] 可选地，在本实施例中，上述电子装置可以位于计算机网络的多个网络设备中的至少一个网络设备。

[0146] 可选地，在本实施例中，上述处理器可以被设置为通过计算机程序执行以下步骤：

[0147] S1，在应用客户端中获取基于目标网页页面触发的网络数据访问请求，其中，网络数据访问请求用于请求访问目标资源数据；

[0148] S2，响应网络数据访问请求，向服务器发送加密数据获取请求，其中，加密数据获取请求用于请求从服务器获取对网络数据访问请求进行加密的加密信息；

[0149] S3，获取服务器响应加密数据获取请求所返回的加密信息；

[0150] S4，利用加密信息对网络数据访问请求进行加密，得到加密后的网络数据访问请求，并将加密后的网络数据访问请求发送至服务器；

[0151] S5，在服务器利用与加密信息匹配的解密信息解密网络数据访问请求，且获取到目标资源数据的情况下，获取服务器返回的数据访问结果，其中，数据访问结果中携带有目标资源数据。

[0152] 可选地，在本实施例中，上述处理器可以被设置为通过计算机程序执行以下步骤：

[0153] S1，在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收应用客户端发送的加密数据获取请求，其中，网络数据访问请求用于请求访问目标资源数据，加密数据获取请求用于请求获取对网络数据访问请求进行加密的加密信息；

[0154] S2，生成加密信息，并将加密信息发送给应用客户端，以使应用客户端利用加密信息对网络数据访问请求进行加密，得到加密后的网络数据访问请求；

[0155] S3，接收应用客户端发送的加密后的网络数据访问请求；

[0156] S4，在利用与加密信息匹配的解密信息解密网络数据访问请求的情况下，获取数

据访问结果，并将数据访问结果发送给应用客户端，其中，数据访问结果中携带有目标资源数据。

[0157] 可选地，本领域普通技术人员可以理解，图11所示的结构仅为示意，电子装置也可以是智能手机(如Android手机、iOS手机等)、平板电脑、掌上电脑以及移动互联网设备(Mobile Internet Devices，MID)、PAD等终端设备。图11其并不对上述电子装置的结构造成限定。例如，电子装置还可包括比图11中所示更多或者更少的组件(如网络接口等)，或者具有与图11所示不同的配置。

[0158] 其中，存储器1102可用于存储软件程序以及模块，如本发明实施例中的数据传输方法对应的程序指令，处理器1104通过运行存储在存储器1102内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的数据传输方法。存储器1102可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器1102可进一步包括相对于处理器1104远程设置的存储器，这些远程存储器可以通过网络连接至终端。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。其中，存储器1102具体可以但不限于用于存储数据访问请求以及目标资源数据等信息。

[0159] 根据本发明的实施例的又一方面，还提供了一种计算机可读的存储介质，该计算机可读的存储介质中存储有计算机程序，其中，该计算机程序被设置为运行时执行上述任一项方法实施例中的步骤。

[0160] 可选地，在本实施例中，上述计算机可读的存储介质可以被设置为存储用于执行以下步骤的计算机程序：

[0161] S1，在应用客户端中获取基于目标网页页面触发的网络数据访问请求，其中，网络数据访问请求用于请求访问目标资源数据；

[0162] S2，响应网络数据访问请求，向服务器发送加密数据获取请求，其中，加密数据获取请求用于请求从服务器获取对网络数据访问请求进行加密的加密信息；

[0163] S3，获取服务器响应加密数据获取请求所返回的加密信息；

[0164] S4，利用加密信息对网络数据访问请求进行加密，得到加密后的网络数据访问请求，并将加密后的网络数据访问请求发送至服务器；

[0165] S5，在服务器利用与加密信息匹配的解密信息解密网络数据访问请求，且获取到目标资源数据的情况下，获取服务器返回的数据访问结果，其中，数据访问结果中携带有目标资源数据。

[0166] 可选地，在本实施例中，上述计算机可读的存储介质可以被设置为存储用于执行以下步骤的计算机程序：

[0167] S1，在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收应用客户端发送的加密数据获取请求，其中，网络数据访问请求用于请求访问目标资源数据，加密数据获取请求用于请求获取对网络数据访问请求进行加密的加密信息；

[0168] S2，生成加密信息，并将加密信息发送给应用客户端，以使应用客户端利用加密信息对网络数据访问请求进行加密，得到加密后的网络数据访问请求；

[0169] S3，接收应用客户端发送的加密后的网络数据访问请求；

[0170] S4，在利用与加密信息匹配的解密信息解密网络数据访问请求的情况下，获取数

据访问结果，并将数据访问结果发送给应用客户端，其中，数据访问结果中携带有目标资源数据。

[0171] 可选地，在本实施例中，本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器(Read-Only Memory，ROM)、随机存取器(Random Access Memory，RAM)、磁盘或光盘等。

[0172] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0173] 上述实施例中的集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在上述计算机可读取的存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在存储介质中，包括若干指令用以使得一台或多台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。

[0174] 在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0175] 在本申请所提供的几个实施例中，应该理解到，所揭露的客户端，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0176] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0177] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0178] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

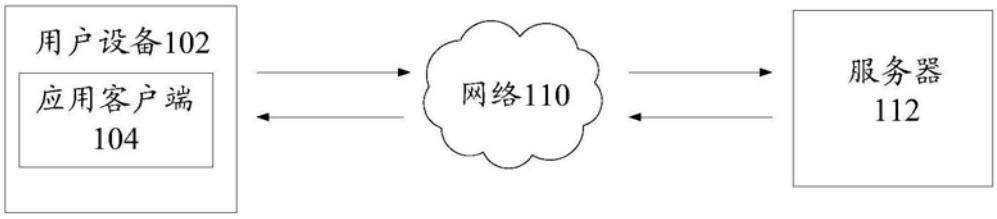

用户设备102
应用客户端
104
网络110
服务器
112

图1

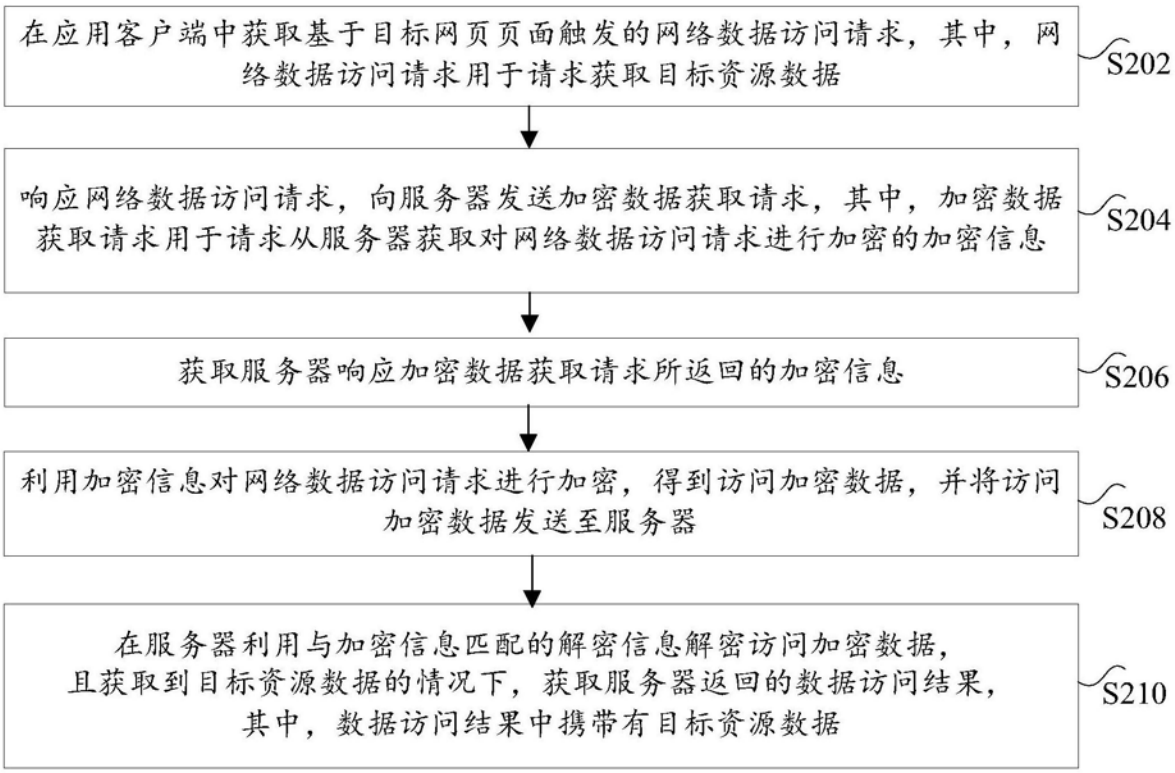

在应用客户端中获取基于目标网页页面触发的网络数据访问请求，其中，网络数据访问请求用于请求获取目标资源数据
S202
响应网络数据访问请求，向服务器发送加密数据获取请求，其中，加密数据获取请求用于请求从服务器获取对网络数据访问请求进行加密的加密信息
S204
获取服务器响应加密数据获取请求所返回的加密信息
S206
利用加密信息对网络数据访问请求进行加密，得到访问加密数据，并将访问加密数据发送至服务器
S208
在服务器利用与加密信息匹配的解密信息解密访问加密数据，且获取到目标资源数据的情况下，获取服务器返回的数据访问结果，其中，数据访问结果中携带有目标资源数据
S210

图2

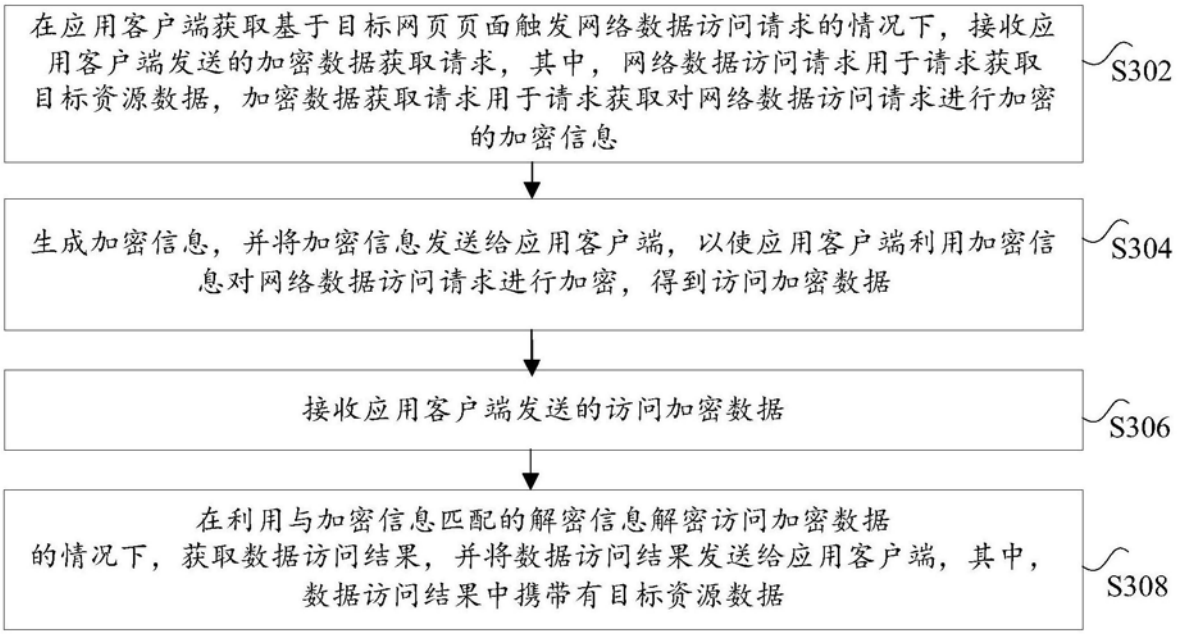

在应用客户端获取基于目标网页页面触发网络数据访问请求的情况下，接收应用客户端发送的加密数据获取请求，其中，网络数据访问请求用于请求获取目标资源数据，加密数据获取请求用于请求获取对网络数据访问请求进行加密的加密信息
S302
生成加密信息，并将加密信息发送给应用客户端，以使应用客户端利用加密信息对网络数据访问请求进行加密，得到访问加密数据
S304
接收应用客户端发送的访问加密数据
S306
在利用与加密信息匹配的解密信息解密访问加密数据的情况下，获取数据访问结果，并将数据访问结果发送给应用客户端，其中，数据访问结果中携带有目标资源数据
S308

图3

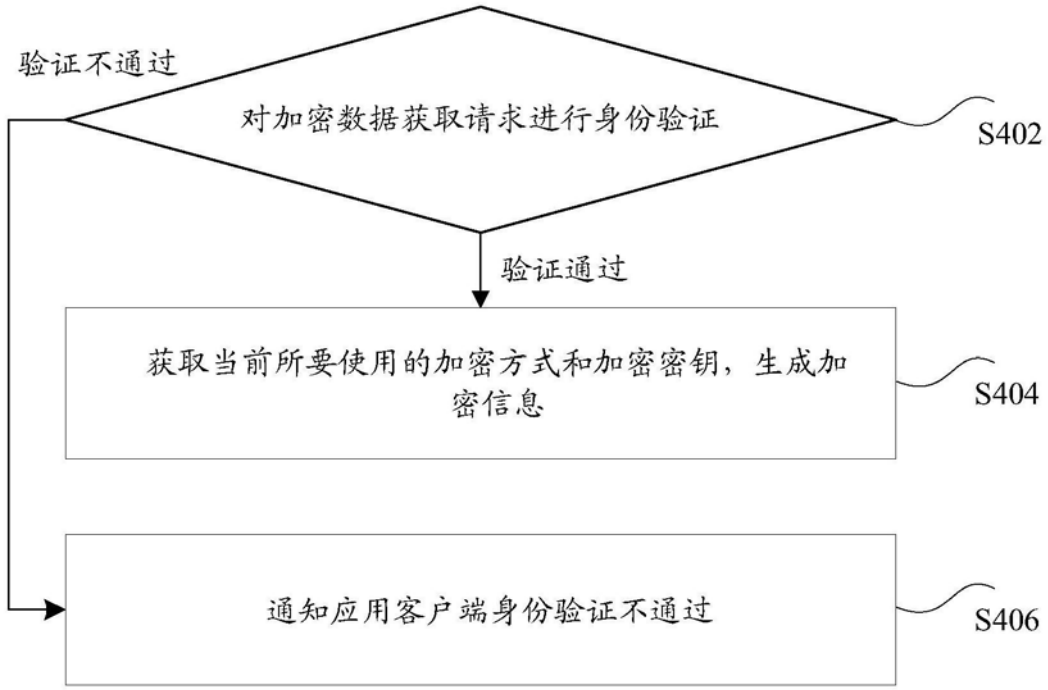

对加密数据获取请求进行身份验证
S402
验证不通过
验证通过
获取当前所要使用的加密方式和加密密钥，生成加密信息
S404
通知应用客户端身份验证不通过
S406

图4

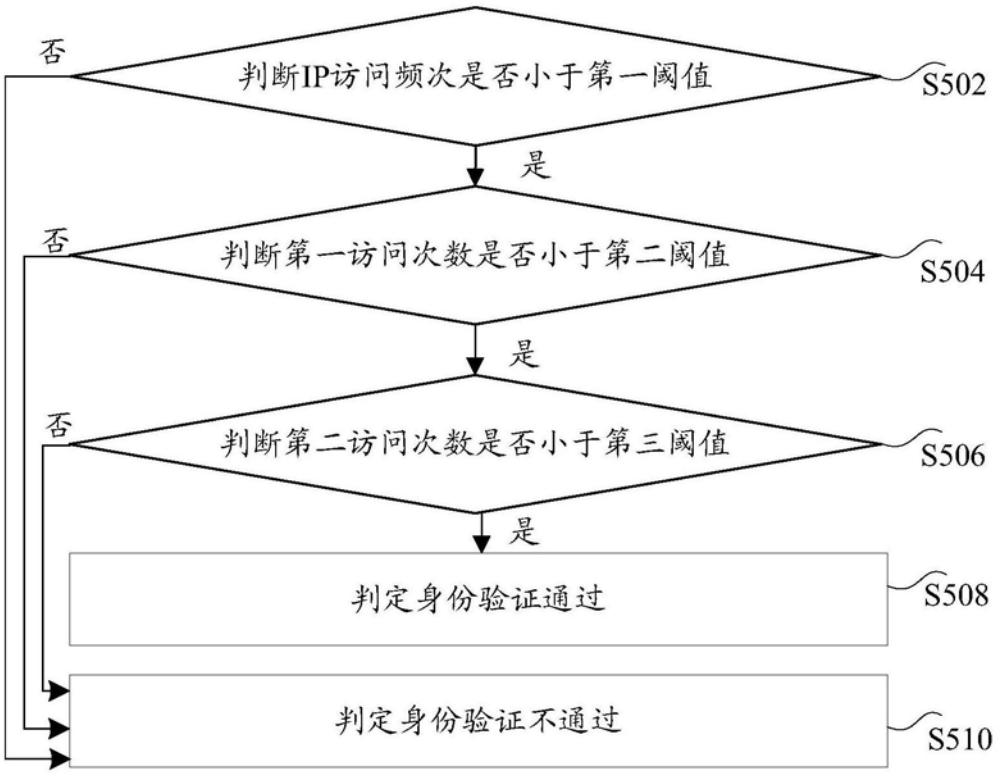

否
判断IP访问频次是否小于第一阈值
S502
是
否
判断第一访问次数是否小于第二阈值
S504
是
否
判断第二访问次数是否小于第三阈值
S506
是
判定身份验证通过
S508
判定身份验证不通过
S510

图5

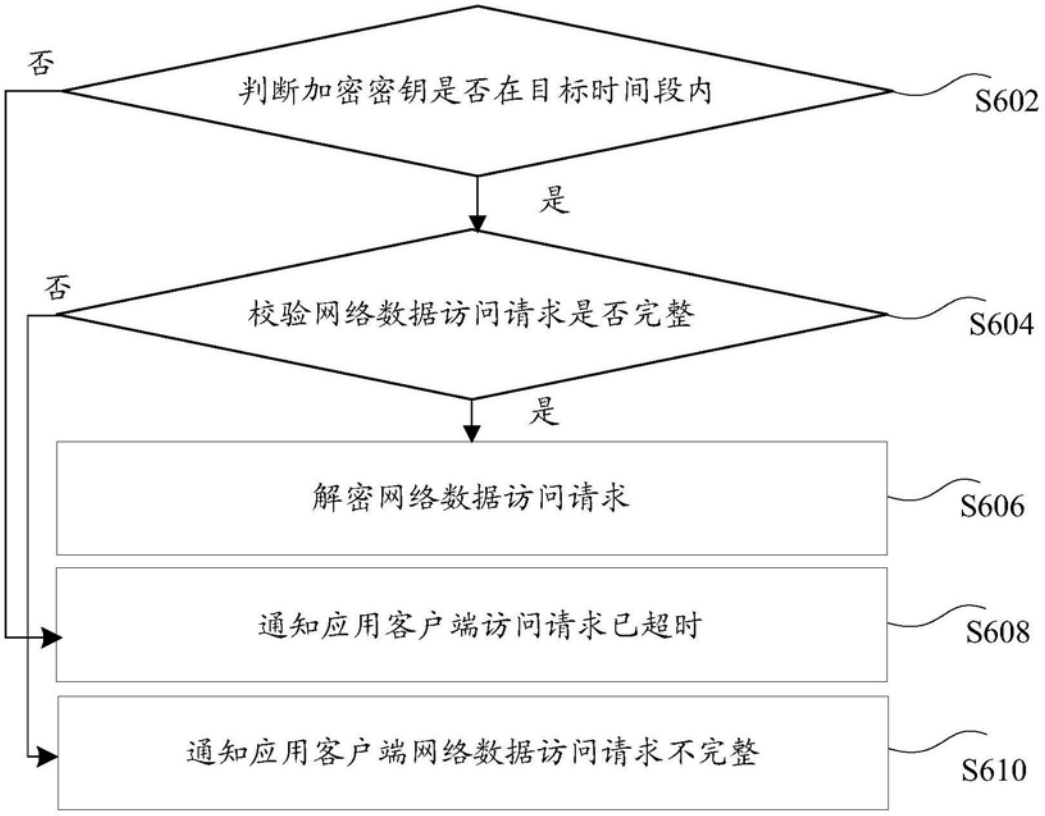

否
判断加密密钥是否在目标时间段内
S602
是
否
校验网络数据访问请求是否完整
S604
是
解密网络数据访问请求
S606
通知应用客户端访问请求已超时
S608
通知应用客户端网络数据访问请求不完整
S610

图6

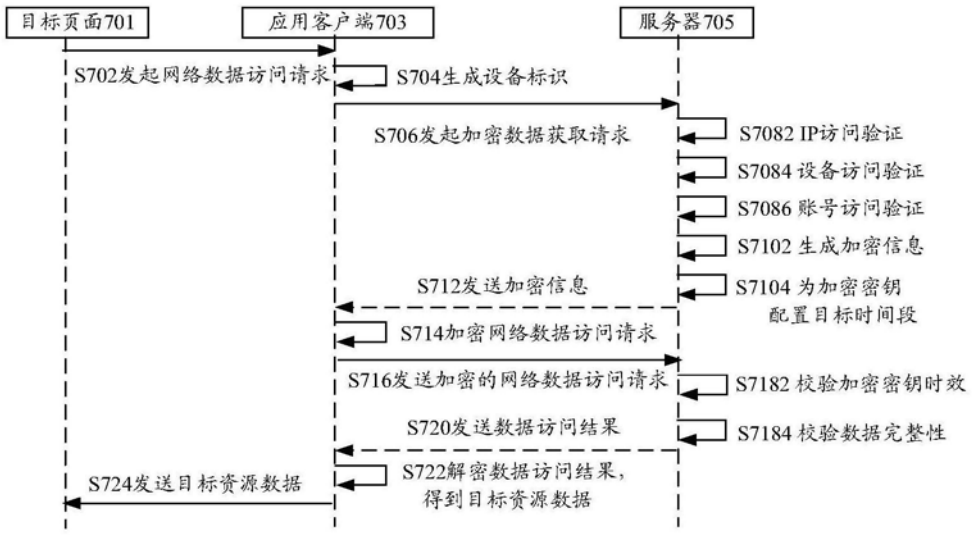

目标页面701
应用客户端703
服务器705
S702发起网络数据访问请求
S704生成设备标识
S706发起加密数据获取请求
S7082 IP访问验证
S7084 设备访问验证
S7086 账号访问验证
S7102 生成加密信息
S712发送加密信息
S7104 为加密密钥
配置目标时间段
S714加密网络数据访问请求
S716发送加密的网络数据访问请求
S7182 校验加密密钥时效
S720发送数据访问结果
S7184 校验数据完整性
S722解密数据访问结果，
得到目标资源数据
S724发送目标资源数据

图7

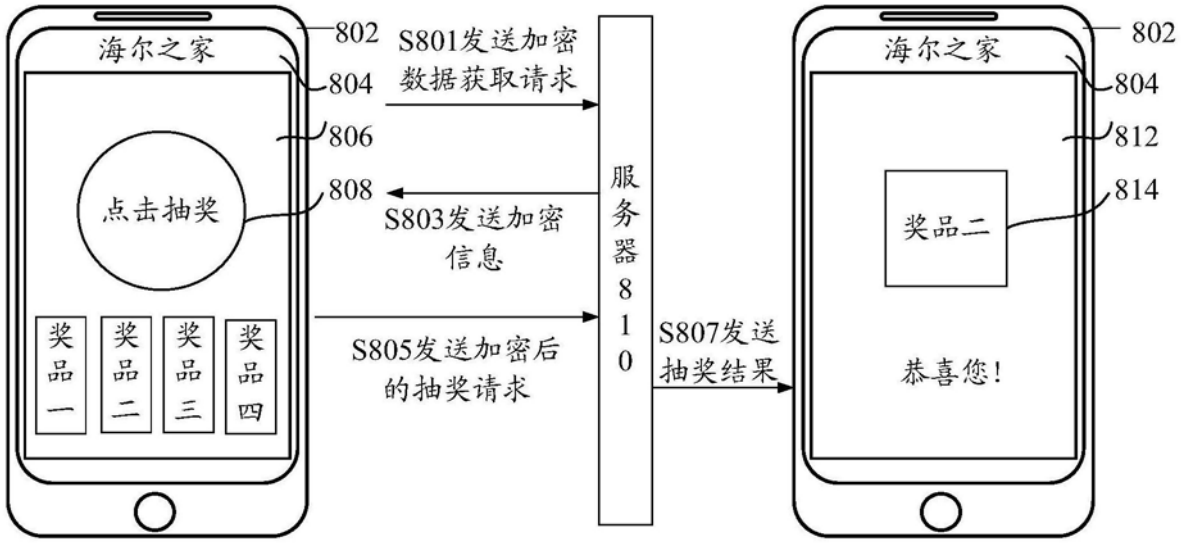

海尔之家
802
804
806
808
点击抽奖
奖品一
奖品二
奖品三
奖品四
S801发送加密数据获取请求
S803发送加密信息
S805发送加密后的抽奖请求
服务器810
S807发送抽奖结果
海尔之家
802
804
812
814
奖品二
恭喜您!

图8

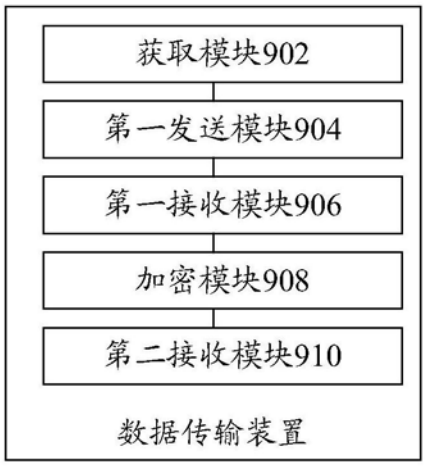

获取模块902
第一发送模块904
第一接收模块906
加密模块908
第二接收模块910
数据传输装置

图9


第一接收模块1002
生成模块1004
第二接收模块1006
处理模块1008
数据传输装置

图10

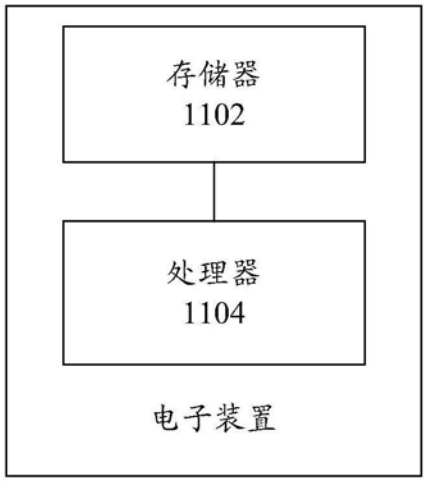


图11