(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 108965311 A
(43)申请公布日 2018.12.07

(21)申请号 201810851516.5

(22)申请日 2018.07.27

(71)申请人 平安科技(深圳)有限公司
地址 518000 广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼

(72)发明人 张驰

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

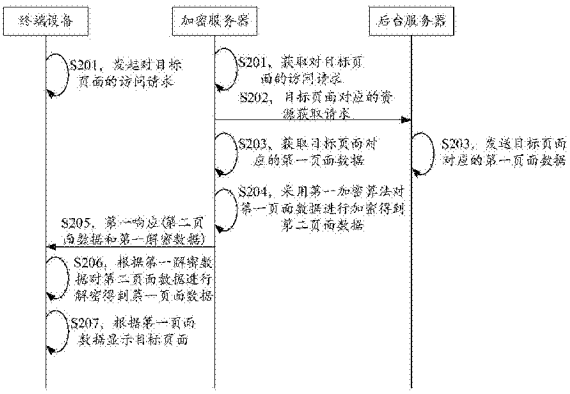
权利要求书2页 说明书11页 附图3页

(54)发明名称

通信数据加密方法和装置

(57)摘要

本发明公开了通信数据加密方法和装置，其中，方法包括：获取终端设备发起的对目标页面的访问请求；根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法对应的解密数据。通过对后台服务器返回的页面数据进行加密，避免扫描器等通用扫描工具直接获取到页面数据，提高后台服务器的安全性。



CN 108965311 A

1.一种通信数据加密方法，其特征在于，包括：

获取终端设备发起的对目标页面的访问请求；

根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

2.根据权利要求1所述的方法，其特征在于，所述第一解密数据包括第一加密算法对应的解密脚本，所述解密脚本被所述终端设备运行时使终端设备执行所述第一加密算法以进行解密；

所述向所述终端设备发送对所述访问请求的第一响应包括：

确定所述第一加密算法对应的解密脚本；

在所述第二页面数据中插入所述第一加密算法对应的解密脚本，并将插入所述第一加密算法对应的解密脚本后的第二页面数据携带在所述第一响应中发送给所述终端设备。

3.根据权利要求1或2所述的方法，其特征在于，在所述目标页面为参数获取页面的情况下，所述第一响应还包括第一加密数据，所述第一加密数据为包含第二加密算法的数据。

4.根据权利要求3所述的方法，其特征在于，所述向所述终端设备发送对所述访问请求的第一响应之后，还包括：

获取所述终端设备发起的参数提交请求，所述参数提交请求包括第一参数，所述第一参数为所述终端设备根据所述第一加密数据对第二参数进行加密得到的参数，所述第二参数为所述终端设备通过所述目标页面获取到的参数；

对所述第一参数进行解密得到所述第二参数；

将所述第二参数发送给所述后台服务器。

5.根据权利要求4所述的方法，其特征在于，所述对所述第一参数进行解密得到所述第二参数包括：

根据所述参数提交请求确定所述终端设备的标识信息；

根据所述终端设备的标识信息确定所述第一加密数据；

根据所述第一加密数据确定所述第二加密算法；

采用所述第二加密算法对所述第一参数进行解密得到所述第二参数。

6.根据权利要求4或5所述的方法，其特征在于，所述将所述第二参数发送给所述后台服务器之后还包括：

获取所述后台服务器根据所述第二参数返回的第三页面数据；

采用第三加密算法对所述第三页面数据进行加密得到第四页面数据；

向所述终端设备发送对所述参数提交请求的第二响应，以使所述终端设备根据第二解密数据对所述第四页面数据进行解密得到所述第三页面数据，所述第二响应包括所述第四页面数据和所述第二解密数据，所述第二解密数据为包含所述第三加密算法的数据。

7.根据权利要求6所述的方法，其特征在于，所述将所述第二参数发送给所述后台服务器包括：

基于安全套接字层的超文本传输HTTPS协议将所述第二参数发送给所述后台服务器。

所述获取所述后台服务器根据所述第二参数返回的第三页面数据包括：

获取所述后台服务器根据所述第二参数基于所述HTTPS协议返回的第三页面数据。

8.一种通信数据加密装置，其特征在于，包括：

访问请求获取模块，用于获取终端设备发起的对目标页面的访问请求；

页面数据获取模块，用于根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

加密模块，用于采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

请求响应模块，用于向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

9.一种通信数据加密装置，包括处理器、存储器以及通信接口，所述处理器、存储器和通信接口相互连接，其中，所述通信接口用于传输数据，所述存储器用于存储程序代码，所述处理器用于调用所述程序代码，执行如权利要求1-7任一项所述的方法。

10.一种计算机存储介质，其特征在于，所述计算机存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行如权利要求1-7任一项所述的方法。

通信数据加密方法和装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及通信数据加密方法和装置。

背景技术

[0002] 网站是依赖于web技术建立的应用，网站应用中的每一次信息交换都涉及web客户端和web服务端，其中，web客户端的主要任务是向用户展现信息内容，其具体利用html语言、脚本程序、CSS、插件技术等实现对应的web页面展示；web服务端为web客户端提供业务支持，其具体利用PHP、ASP、JSP等技术实现相应的功能。web服务端和web客户端的交互流程一般为：web客户端向web服务端发送请求，web服务端基于web客户端发出的请求向web客户端返回该请求对应的数据(如html代码等)。

[0003] 为了提高网站的安全性，一般会采用一定的加密技术对网站的某些数据进行加密，在目前的一些加密设计中，主要是通过对网站的html代码进行加密以避免网站的内容结构被轻易读取。但是，目前还有一些网站的各个功能之间的交互参数(如通过post表单提交的用户名、密码等)是以明文的形式进行传输，面临被监听的风险，网站的安全性不够高。

发明内容

[0004] 本发明实施例提供通信数据加密方法和装置，解决网站安全性不够高的问题。

[0005] 第一方面，提供一种通信数据加密方法，包括：

[0006] 获取终端设备发起的对目标页面的访问请求；

[0007] 根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

[0008] 采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

[0009] 向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

[0010] 本发明实施例中，通过将终端设备向服务器发起的访问请求所对应的页面数据进行加密，并将加密方式所对应的解密数据连同加密后的页面数据一起发送给终端设备，确保终端设备可以采用该解密数据对加密后的页面数据进行解密从而显示该访问请求对应的目标页面，通过将页面数据加密的方式对后台服务器向终端设备返回的数据进行加密，可以避免扫描器、爬虫工具等扫描页面的工具直接获取到页面数据，增加了网站的安全性。

[0011] 结合第一方面，在一种可能的实现方式中，所述第一解密数据包括第一加密算法对应的解密脚本，所述解密脚本被终端设备运行时使所述终端设备执行所述第一加密算法以进行解密；所述向所述终端设备发送对所述访问请求的第一响应包括：确定所述第一加密算法对应的解密脚本；在所述第二页面数据中插入所述第一加密算法对应的解密脚本，并将插入所述第一加密算法对应的解密脚本后的第二页面数据携带在所述第一响应中发送给所述终端设备。通过将加密页面数据时使用的加密方式所对应的解密脚本插入在加密

后的页面数据中，使得终端设备可以运行该解密脚本以进行该解密脚本对应的运算，从而可以对加密后的页面数据进行解密。

[0012] 结合第一方面，在一种可能的实现方式中，在所述目标页面为参数获取页面的情况下，所述第一响应还包括第一加密数据，所述第一加密数据为第二加密算法对应的数据。通过在向终端设备返回的响应中加入加密方式对应的数据，使得终端设备可以根据该加密数据对需要向后台服务器提交的数据进行加密。

[0013] 结合第一方面，在一种可能的实现方式中，所述向所述终端设备发送对所述访问请求的第一响应之后，还包括：获取所述终端设备发起的参数提交请求，所述参数提交请求包括第一参数，所述第一参数为所述终端设备根据所述第一加密数据对第二参数进行加密得到的参数，所述第二参数为所述终端设备通过所述目标页面获取到的参数；对所述第一参数进行解密得到所述第二参数，将所述第二参数发送给所述后台服务器。由于事先将加密数据发送给终端设备，使得终端设备可以对提交的参数进行加密，通过对终端设备向后台服务器提交的参数进行加密，避免扫描器、爬虫工具等扫描工具获取到这些参数，增加了终端设备与后台服务器之间的交互数据的安全性。

[0014] 结合第一方面，在一种可能的实现方式中，所述对所述第一参数进行解密得到所述第二参数包括：根据所述参数提交请求确定所述终端设备的标识信息；根据所述终端设备的标识信息确定所述第一加密数据；根据所述第一加密数据确定所述第二加密算法；采用所述第二加密算法对所述第一参数进行解密得到所述第二参数。通过确定终端设备的身份，可确定之前发送给终端设备的加密数据，从而可以根据该加密数据确定终端设备加密参数时所采用的加密方式，进而可以对加密后的参数进行解密。

[0015] 结合第一方面，在一种可能的实现方式中，所述将所述第二参数发送给所述后台服务器之后还包括：获取所述后台服务器根据所述第二参数返回的第三页面数据；采用第三加密算法对所述第三页面数据进行加密得到第四页面数据；向所述终端设备发送对所述参数提交请求的第二响应，以使所述终端设备根据第二解密数据对所述第四页面数据进行解密得到所述第三页面数据，所述第二响应包括所述第四页面数据和所述第二解密数据，所述第二解密数据为包含所述第三加密算法的数据。

[0016] 结合第一方面，所述将所述第二参数发送给所述后台服务器包括：基于安全套接字层的超文本传输协议(hypertext transfer protocol over secure socket layer，HTTPS)将所述第一参数发送给所述后台服务器；所述获取所述后台服务器根据所述第二参数返回的第三页面数据包括：获取所述后台服务器根据所述第二参数基于所述HTTPS协议返回的第三页面数据。在与后台服务器进行交互时，基于HTTPS协议进行传输，确保与后台服务器之间交互的数据是加密的，从而保证交互数据在整个传输的过程中都是加密的。

[0017] 第二方面，提供一种通信数据加密装置，包括：

[0018] 访问请求获取模块，用于获取终端设备发起的对目标页面的访问请求；

[0019] 页面数据获取模块，用于根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

[0020] 加密模块，用于采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

[0021] 请求响应模块，用于向所述终端设备发送对所述访问请求的第一响应，以使所述

终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

[0022] 第三方面，提供另一种通信数据加密装置，包括处理器、存储器以及通信接口，所述处理器、存储器和通信接口相互连接，其中，所述通信接口用于接收或发送数据，所述存储器用于存储通信数据加密装置执行上述方法的应用程序代码，所述处理器被配置用于执行上述第一方面的方法。

[0023] 第四方面，提供一种计算机存储介质，所述计算机存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行上述第一方面的方法。

[0024] 本发明实施例中，通过截获终端设备与后台服务器之间交互的数据并对其进行加密，保证了终端设备与后台服务器之间交互的数据的安全性。

附图说明

[0025] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0026] 图1是本发明实施例提供的一种网站系统的架构示意图；

[0027] 图2是本发明实施例提供的一种通信数据加密方法的流程示意图；

[0028] 图3是本发明实施例提供的另一种通信数据加密方法的流程示意图；

[0029] 图4是本发明实施例提供的一种通信数据加密装置的组成结构示意图；

[0030] 图5是本发明实施例提供的另一种通信数据加密装置的组成结构示意图。

具体实施方式

[0031] 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，所描述的实施例仅是本发明一部分实施例，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，都属于本发明保护的范围。

[0032] 本发明的技术方案适用于传统的以明文形式传输数据的网站系统，网站系统可包括网站客户端和网站服务端。网站客户端为面向用户的客户端，用于为用户提供服务。该网站客户端可以是通用型的客户端，通用型的客户端可以为多个网站服务器提供服务，例如可以为浏览器；该网站客户端也可以特定的客户端，该特定的客户端只用于为某个特定网站提供服务，例如为“腾讯视频”客户端。一般情况下，该网站客户端运行在用户的终端设备上，其中，终端设备包括但不限于手机、电脑、平板电脑、电子阅读器等具备网站浏览功能的电子设备。网站服务端用于管理并向网站客户端提供该网站系统的资源，网站服务端用于向网站客户端提供各种数据使得该网站客户端可以向用显示各种页面。该网站服务端可以由一台或多台服务器组成。本发明实施例通过在传统的以明文形式传输数据的网站系统中增加加密服务器，利用加密服务器对网站服务端与网站客户端之间交互的数据加密，以实

现保障网站安全的目的。示例性地，本发明实施例的网站系统的架构可以如图1所示，网站系统包括运行在终端设备101上的网站客户端、加密服务器102以及网站服务器103，其中，加密服务器102用于获取网站客户端与加密网站服务端之间的交互数据并进行加密。

[0033] 本发明实施例的方法可以实现在图1所示的系统架构上，下面介绍本发明实施例的方法。

[0034] 参见图2，图2是本发明实施例提供的一种通信数据加密方法的流程示意图，如图所示，该方法包括：

[0035] S201，终端设备发起对目标页面的访问请求，加密服务器获取对目标页面的访问请求。

[0036] 这里，终端设备通过运行在终端设备中的网站客户端发起对目标页面的访问请求，该目标页面为网站系统的其中一个页面。在该网站客户端为通用型的客户端的情况下，该目标页面可以为用户想要访问的任意一个网站系统的其中一个页面；在该网站客户端为特定的客户端的情况下，该目标页面为该网站客户端对应的网站系统的其中一个页面。

[0037] 该目标页面对应一个统一资源定位符(uniform resource location，URL)，该访问请求携带该URL，该URL指向一个互联网协议(Internet protocol，IP)地址，该IP地址为该访问请求访问的地址。

[0038] 本发明实施例中，该URL指向的IP地址可以有以下两种设计：

[0039] 第一种设计，该URL指向的IP地址为加密服务器的IP地址。当终端设备发起对该目标页面的访问请求时，终端设备对该URL进行域名解析系统(domain name system，DNS)解析得到的IP地址为该加密服务器的IP地址。终端设备根据该加密服务器的IP地址向加密服务器发起对目标页面的访问请求，加密服务器通过接收的方式获取该对目标页面的访问请求。

[0040] 第二种设计，该URL指向的IP地址为后台服务器的IP地址。当终端设备发起对该目标页面的访问请求时，终端设备对该URL进行DNS解析得到的IP地址为该后台服务器的IP地址。终端设备根据该后台服务器的IP地址向后台服务器发起对目标页面的访问请求，加密服务器通过流量劫持的方式截取该对目标页面的访问请求从而获取该对目标页面的访问请求。

[0041] S202，加密服务器向后台服务器发送目标页面对应的资源获取请求，后台服务器接收对目标页面的资源访问请求。

[0042] 这里，后台服务器为该目标页面对应的后台服务器，也即包含该目标页面的网站系统的后台服务器。目标页面对应的资源获取请求用于请求该后台服务器返回该目标页面对应的第一页面数据，该第一页面数据被终端设备中的网站客户端运行时可以使得该网站客户端显示该目标页面。

[0043] 本发明实施例中，加密服务器向后台服务器发送目标页面对应的资源获取请求有以下两种情况：

[0044] 第一种情况，在对目标页面的访问请求中携带的URL指向的IP地址为上述第一种设计的情况下，可以在加密服务器中预置该后台服务器的IP地址，并将后台服务器的IP地址与目标访问请求关联，当加密服务器获取到目标访问请求时，根据与该目标访问请求关联的IP地址确定该目标访问请求对应的页面数据的资源在该后台服务器上，从而加密服务

器可以根据与该目标访问请求对应的IP地址向该后台服务器发起目标页面对应的资源获取请求，其中，目标访问请求是指与该后台服务器关联的访问请求，即该网站系统的相关请求。

[0045] 例如，预先将“pingan.com”这一域名与后台服务器的IP地址相对应，后台服务器的IP地址为192.168.11.32，当加密服务器接收到访问请求中携带“pingan.com”这一域名的请求时，例如为www.pingan.com/login，由于这个请求中携带有“pingan.com”，则可以确定与这个请求对应的后台服务器的IP地址为192.168.11.32，则加密服务器向IP地址为192.168.11.32的后台服务器发起该访问请求对应的资源请求。

[0046] 第二种情况，在目标页面的访问请求中携带的URL指向的IP地址为上述第二种设计的情况下，加密服务器在截取到该对目标页面的访问请求后，可以对该访问请求中的携带的URL进行DNS解析得到该后台服务器的IP地址，加密服务器可以根据解析得到的后台服务器的IP地址向后台服务器发起目标页面对应的资源获取请求。具体地，该目标页面对应的资源获取请求可以为该对目标页面的访问请求。

[0047] 例如，加密服务器截取到的访问请求中携带的URL为www.pingan.com/login，加密服务器通过DNS方式解析该URL得到该URL对应的IP地址为202.132.11.32，则加密服务器向IP地址为202.132.11.32的服务器发起目标页面对应的资源请求。

[0048] S203，后台服务器发送目标页面对应的第一页面数据，加密服务器获取目标页面对应的第一页面数据。

[0049] 这里，后台服务器根据该目标页面对应的资源获取请求从网站目录中找到该目标页面对应的网站文件，从该网站文件中获取第一页面数据，然后发送该第一页面数据。

[0050] 本发明实施例中，在该访问请求中携带的URL为上述第一种设计的情况下，后台服务器向该加密服务器发送目标页面对应的第一页面数据，加密服务器通过接收的方式获取目标页面对应的第一页面数据；在该访问请求中携带的URL为上述第二种设计的情况下，后台服务器向该终端设备发送目标发送页面对应的第一页面数据，该加密服务器通过流量劫持的方式截取该对目标页面对应的第一页面数据。

[0051] 可选地，如果该访问请求中携带的URL为上述第一种设计，在第一种可能的实现方式中，加密服务器与后台服务器可以基于HTTPS协议进行通信。其中，加密服务器可以基于HTTPS协议向后台服务器发送目标页面对应的资源获取请求，加密服务器可以基于HTTPS协议向加密服务器发送该目标页面对应的第一页面数据。在第二种可能的实现方式中，该加密服务器的访问方式可以为只允许加密服务器访问，即该后台服务器的访问白名单中有且只有该加密服务器的IP地址或MAC地址等证明该加密服务器的身份信息。以一种安全的方式保证加密服务器与后台服务器之间的交互过程的通信安全，进一步增强了网站系统的安全性。

[0052] S204，加密服务器采用第一加密算法对第一页面数据进行加密得到第二页面数据。

[0053] 本发明实施例中，第一加密算法可以是对称算法，也可以是非对称算法，其中，第一加密算法包括但不限于数据加密标准(data encryption standard，DES)算法、3DES算法、RSA算法、高级加密标准(advanced encryption standard，AES)算法。

[0054] 具体实现中，加密服务器从第一加密算法对应的密钥空间中选择其中一个密钥作

为第一密钥，对该第一密钥和该第一页面数据进行该第一加密算法对应的运算，得到第二页面数据。

[0055] S205，加密服务器向终端设备发送第一响应，终端设备接收第一响应，第一响应包括第二页面数据和第一解密数据。

[0056] 这里，第一响应为对步骤S201的访问请求的响应。第一解密数据可以包括两部分数据，第一部分数据为第二密钥，第二部分数据为使该终端设备进行该第一加密算法对应的运算的数据。在该第一加密算法为对称算法的情况下，该第二密钥与加密服务器对该第一页面数据进行加密时所使用的密钥相同，即该第二密钥为加密服务器对该第一页面数据进行加密时所使用的密钥；在该第一加密算法为非对称算法的情况下，如果加密服务器对该第一页面数据进行加密时所使用的第一密钥为公钥，则该第二密钥为该公钥对应的私钥，如果该加密服务器对该第一页面数据进行加密时所使用的第一密钥为私钥，则该第二密钥为该私钥对应的公钥。

[0057] 在一种可能的方式中，该使终端设备进行与该第一加密算法对应的运算的数据可以为该第一加密算法对应的解密脚本，则该加密服务器向终端设备发送第一响应可以如下：加密服务器确定第一加密算法对应的解密脚本；加密服务器在第二页面数据中插入该第一加密算法对应的解密脚本，并将插入第一加密算法对应的解密脚本后的第二页面数据携带在第一响应中发送给终端设备。

[0058] 具体实现中，可以在加密服务器预置至少一种加密算法(指执行该加密算法的计算机程序)，并且在加密服务器中预置密钥空间、加密脚本以及解密脚本，然后将密钥空间、加密脚本、解密脚本与加密算法对应。在发送第一响应时，加密服务器可以选择与加密算法对应的解密脚本发送给终端设备，以下进行具体说明：

[0059] 第一种情况，在加密服务器中预置一种加密算法。在这种情况下，加密服务器中加密算法对应的加密脚本和解密脚本均只有一个，加密服务器获取该唯一的解密脚本，在第二页面数据中插入该唯一的解密脚本，然后将插入解密脚本后的第二页面数据以及第二密钥发送给终端设备。

[0060] 第二种情况，加密服务器中预置有多种加密算法。在这种情况下，加密服务器中加密算法有多种，加密脚本和解密脚本有多个，加密服务器可以根据加密算法与加密脚本以及解密脚本相互之间的对应关系选择与第一加密算法对应的解密脚本作为目标解密脚本，然后在第二页面数据中插入该目标解密脚本，然后将插入目标解密脚本后的第二页面数据以及第二密钥发送给终端设备。

[0061] S206，终端设备根据第一解密数据对第二页面数据进行解密得到第一页面数据。

[0062] 具体实现中，终端设备从第一解密数据中分别获取第二密钥和使终端设备进行与该第一加密算法对应的运算的数据，然后通过该使终端设备进行与第一加密算法的运算的数据对该第二密钥和该第二页面数据进行该第一加密算法对应的运算，运算得到的数据为第一页面数据。

[0063] 在使终端设备进行与该第一加密算法对应的运算的数据为第一加密算法对应的解密脚本的情况下，终端设备运行该第一加密算法对应的解密脚本对该第二密钥和该第二页面数据进行该第一加密算法对应的运算得到第一页面数据。

[0064] S207，终端设备根据第一页面数据显示目标页面。

[0065] 本发明实施例中，加密服务器通过将终端设备向服务器发起的访问请求所对应的页面数据进行加密，并将加密方式所对应的解密数据连同加密后的页面数据一起发送给终端设备，使得终端设备可以采用该解密数据对加密后的页面数据进行解密从而能够显示该访问请求对应的目标页面，通过将页面数据加密的方式对后台服务器向终端设备返回的数据进行加密，避免了扫描器、爬虫工具等通用扫描工具能够直接获取到页面数据而获取到网站的信息，增加了后台服务器的安全性。

[0066] 在上述图2对应的实施例中，加密服务器对后台服务器向终端设备返回的页面数据进行了加密，在一些可能的实现方式中，如果该目标页面为参数获取页面，在终端设备向后台服务器提交从目标页面获取到的参数信息的情况下，终端设备可以对终端设备向后台服务器提交的参数信息进行加密。加密服务器可以将用于加密该参数信息的加密数据携带在该目标页面对应的页面数据中发送给终端设备，即在该目标页面为参数页面获取页面的情况下，该第一响应还可以包括第一加密数据，该第一加密数据为包含第二加密算法的数据，该第一加密数据可以被终端设备用于加密数据。

[0067] 第一加密数据可以包括两部分数据，第一部分数据为第三密钥，第二部分数据为使该终端设备进行与该第二加密算法对应的运算的数据。

[0068] 第二加密算法可以为对称算法，也可以为非对称算法，在第二加密算法为对称算法的情况下，该第三密钥为对称密钥；在第二加密算法为非对称算法的情况下，该第二加密密钥为非对称密钥。第二加密算法包括但不限于DES算法、3DES算法、RSA算法、AES算法。

[0069] 第二加密算法与第三密钥可以有以下几种情况：

[0070] 一、第二加密算法与第一加密算法相同，第三密钥与第一密钥相同。

[0071] 二、第二加密算法与第一加密算法相同，第三密钥与第一密钥不同。

[0072] 三、第二加密算法与第一加密算法不同，第三密钥与第一密钥相同。

[0073] 四、第二加密算法与第一加密算法不同，第三密钥与第一密钥相同。

[0074] 在上述四种情况中，除第一种情况外，其余三种情况均可以实现对终端设备与后台服务器之间交互的数据的动态加密。

[0075] 在一种可能的实现方式中，该使终端设备进行与该第二加密算法对应的运算的数据可以为该第二加密算法对应的加密脚本，则该加密服务器向终端设备发送第一响应还可以包括：加密服务器确定第二加密算法对应的加密脚本；加密服务器在第二页面数据中插入该第二加密算法对应的解密脚本，然后将插入第一加密算法对应的解密脚本和第二加密算法对应的加密脚本后的第二页面数据携带在第一响应中发送给终端设备。

[0076] 在第一加密算法与第二加密算法为相同的加密算法的情况下，该第二加密算法对应的加密脚本可以与该第一加密算法对应的解密脚本可以为同一个脚本。

[0077] 在将第一加密数据携带在第一响应中发送给终端设备后，终端设备可以利用该第一加密数据对从该目标页面获取到的参数信息进行加密。参见图3，图3是本发明实施例提供的另一种通信数据加密方法的流程示意图，该方法可以在上述步骤S207之后被执行，该方法包括：

[0078] S301，终端设备通过目标页面获取用户输入的第二参数。

[0079] 本发明实施例中，目标页面为参数获取页面，参数获取页面是指用户可以输入数据并进行提交的页面，参数获取页面具体可以为登录页面、用户信息填写页面、用户意见提

交页面，等等。第二参数为用户输入的信息，第二参数可以为用户通过登录页面输入的用户名、密码、验证码等，第二参数也可以为用户通过用户信息填写页面填写的姓名、性别、年龄等，第二参数还可以为用户提交的留言、建议等，不限于这里的描述。

[0080] S302，终端设备根据第一加密数据对第二参数进行加密得到第一参数。

[0081] 具体实现中，终端设备可以从第一加密数据中分别获取第三密钥和使终端设备进行与该第二加密算法对应的运算的数据，然后通过该使终端设备进行与该第二加密算对应的运算的数据对该第三密钥和该第二参数进行该第二加密算法对应的运算，运算得到的数据为第一参数。

[0082] 在使终端设备进行与该第二加密算法对应的运算的数据为第二加密算法对应的加密脚本的情况下，终端设备运行该第二加密算法对应的加密脚本对该第二密钥和该第二参数进行该第二加密算法对应的运算得到第一参数。

[0083] S303，终端设备发起参数提交请求，加密服务器获取参数提交请求，参数提交请求包括第一参数。

[0084] 这里，参数提交请求中携带一个URL，该URL指向一个IP地址，该IP地址为该参数提交请求提交参数的地址。该URL指向的IP地址与访问请求中携带的URL指向的IP地址相同。终端设备发起参数提交请求以及加密服务器获取参数提交请求的具体实现方式可以参考前述终端设备发起访问请求以及加密服务器获取访问请求的描述，此处不再赘述。

[0085] S304，加密服务器对第一参数进行解密得到第二参数。

[0086] 如前所述，第一加密数据由加密服务器发送给终端设备，当获取到该参数提交请求时，该参数提交请求中除了携带第一参数外，还携带终端设备的标识信息，加密服务器可以根据该参数提交请求确定终端设备的标识信息，然后根据终端设备的标识信息确定第一加密数据，根据第一加密数据确定第二加密算法，最后采用该第二加密算法对第一参数进行解密得到第二参数。其中，终端设备的标识信息可以为session信息或者cookie信息。

[0087] 具体实现中，加密服务器在确定了第一加密数据后，在第三加密算法对应的密钥空间中确定与第一加密数据中的第三密钥对应的第四密钥，其中，在第三密钥为对称密钥的情况下，该第四密钥为该第三密钥，在第三密钥为非对称密钥的情况下，如果该第三密钥为公钥，则该第四密钥为该公钥对应的私钥，如果该第三密钥为私钥，则该第四密钥为该私钥对应的公钥；在确定第四密钥后，加密服务器对该第四密钥以及该第一参数进行该第二加密算法算法对应的运算得到第二参数。

[0088] S305，加密服务器将第二参数发送给后台服务器，后台服务器接收第二参数。

[0089] 本发明实施例中，加密服务器将第二参数发送给后台服务器与加密服务器向后台服务器发送目标页面对应的资源获取请求类似，在一种可能的情况中，加密服务器可以根据该参数提交请求确定该参数提交请求对应的IP地址，根据该参数提交请求对应的IP地址向后台服务器发送该第二参数；在另一种可能的情况中，加密服务器对该参数提交请求中的URL进行解析得到该后台服务器的IP地址，然后根据该解析得到的IP地址向后台服务发送该第二参数。

[0090] S306，后台服务器根据第二参数发送第三页面数据，加密服务器获取第三页面数据。

[0091] 这里，后台服务器根据第二参数发送第三页面数据以及加密服务器获取第三页面

数据的方式可参考前述步骤S203后台服务器发送目标页面对应的第一页面数据以及加密服务器获取目标页面对应的第一页面数据的描述，此处不再赘述。

[0092] 可选地，在该参数提交请求携带的URL为上述第一种设计的情况下，在在第一种可能的实现方式中，加密服务器与后台服务器可以基于HTTPS协议进行通信。加密服务器基于HTTPS协议向后台服务器发送第二参数，加密服务器基于HTTPS协议向加密服务器发送该第三页面数据。在第二种可能的实现方式中，该加密服务器的访问方式可以为只允许加密服务器访问。通过安全手段保证加密服务器与后台服务器之间的交互过程的通信安全，进一步增强了网站系统的安全性。

[0093] S307，加密服务器采用第三加密算法对第三页面数据进行加密得到第四页面数据。

[0094] S308，加密服务器向终端设备发送第二响应，终端设备接收第二响应，第二响应包括第四页面数据以及第二解密数据。

[0095] S309，终端设备根据第二解密数据对第四页面数据解密得到第三页面数据。

[0096] S310，终端设备显示第三页面数据对应的页面。

[0097] 这里，步骤S307～S310的具体实现方式与上述步骤S204～S207的具体实现方式类似，可参考前述步骤S204～S207的描述，此处不再赘述。

[0098] 本发明实施例中，加密服务器通过将加密数据携带在参数获取页面对应的页面数据中发送给终端设备，使得终端设备可以采用该加密数据对通过参数获取页面获取到的参数进行加密，从而避免这些参数在传输的过程中被获取到，在不需要改变原有网站架构的情况下保证了参数的安全性和隐私性。

[0099] 上面介绍了发明实施例的方法，下面介绍发明实施例的装置。

[0100] 参见图4，图4是本发明实施例提供的一种通信数据加密装置的组成结构示意图，该装置40可以为上述图1或图2-图3所示的实施例中的加密服务器或加密服务器的一部分，该装置40包括：

[0101] 访问请求获取模块401，用于获取终端设备发起的对目标页面的访问请求；

[0102] 页面数据获取模块402，用于根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据；

[0103] 加密模块403，用于采用第一加密算法对所述第一页面数据进行加密得到第二页面数据；

[0104] 请求响应模块404，用于向所述终端设备发送对所述访问请求的第一响应，以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据，所述第一响应包括所述第二页面数据以及所述第一解密数据，所述第一解密数据为包含所述第一加密算法的数据。

[0105] 在一种可能的设计中，所述第一解密数据包括第一加密算法对应的解密脚本，所述解密脚本被所述终端设备运行时使终端设备执行所述第一加密算法以进行解密；

[0106] 该请求响应模块404具体用于：

[0107] 确定所述第一加密算法对应的解密脚本；

[0108] 在所述第二页面数据中插入所述第一加密算法对应的解密脚本，并将插入所述第一加密算法对应的解密脚本后的第二页面数据携带在所述第一响应中发送给所述终端设

备。

[0109] 在一种可能的设计中，在所述目标页面为参数获取页面的情况下，所述第一响应还包括第一加密数据，所述第一加密数据为包含第二加密算法对应的的数据。

[0110] 在一种可能的设计中，该装置40还包括：

[0111] 提交请求获取模块405，用于获取所述终端设备发起的参数提交请求，所述参数提交请求包括第一参数，所述第一参数为所述终端设备根据所述第一加密数据对第二参数进行加密得到的参数，所述第二参数为所述终端设备通过所述目标页面获取到的参数；

[0112] 解密模块406，用于对所述第一参数进行解密得到所述第二参数；

[0113] 发送模块407，用于将所述第二参数发送给所述后台服务器。

[0114] 在一种可能的设计中，所述解密模块406具体用于：

[0115] 根据所述参数提交请求确定所述终端设备的标识信息；

[0116] 根据所述终端设备的标识信息确定所述第一加密数据；

[0117] 根据所述第一加密数据确定所述第二加密算法；

[0118] 采用所述第二加密算法对所述第一参数进行解密得到所述第二参数。

[0119] 在一种可能的设计中，所述页面数据获取402还用于获取所述后台服务器根据所述第二参数返回的第三页面数据；

[0120] 所述加密模块403还用于采用第三加密算法对所述第三页面数据进行加密得到第四页面数据；

[0121] 所述请求响应模块404还用于向所述终端设备发送对所述参数提交请求的第二响应，以使所述终端设备根据第二解密数据对所述第四页面数据进行解密得到所述第三页面数据，所述第二响应包括所述第四页面数据和所述第二解密数据，所述第二解密数据为包含所述第三加密算法的数据。

[0122] 在一种可能的设计中，所述发送模块407具体用于：基于安全套接字层的超文本传输HTTPS协议将所述第一参数发送给所述后台服务器；

[0123] 所述页面数据获取模块402具体用于获取所述后台服务器基于所述HTTPS协议根据所述第二参数返回的第三页面数据。

[0124] 需要说明的是，图4对应的实施例中未提及的内容可参见方法实施例的描述，这里不再赘述。

[0125] 本发明实施例中，通信数据加密装置通过将终端设备向服务器发起的访问请求所对应的页面数据进行加密，并将加密方式所对应的解密数据连同加密后的页面数据一起发送给终端设备，使得终端设备可以采用该解密数据对加密后的页面数据进行解密从而能够显示该访问请求对应的目标页面，通过将页面数据加密的方式对后台服务器向终端设备返回的数据进行加密，避免了扫描器等通用扫描工具能够直接获取到页面数据而获取到网站的信息，增加了后台服务器的安全性。

[0126] 参见图5，图5是本发明实施例提供的另一种通信数据加密装置的组成结构示意图，该装置可以为上述图1或图2-图3所示的实施例中的加密服务器或加密服务器的一部分，如图所示，该装置50包括处理器501、存储器502以及通信接口503。处理器501连接到存储器502和通信接口503，例如处理器501可以通过总线连接到存储器502和通信接口503。

[0127] 处理器501被配置为支持所述通信数据加密装置执行图2-图3所述的通信数据加

密方法中加密服务器相应的功能。该处理器501可以是中央处理器(Central Processing Unit,CPU),网络处理器(Network Processor,NP),硬件芯片或者其任意组合。上述硬件芯片可以是专用集成电路(Application-Specific Integrated Circuit,ASIC),可编程逻辑器件(Programmable Logic Device,PLD)或其组合。上述PLD可以是复杂可编程逻辑器件(Complex Programmable Logic Device,CPLD),现场可编程逻辑门阵列(Field-Programmable Gate Array,FPGA),通用阵列逻辑(Generic Array Logic,GAL)或其任意组合。

[0128] 存储器502存储器用于存储程序代码等。存储器502可以包括易失性存储器(Volatile Memory,VM),例如随机存取存储器(Random Access Memory,RAM);存储器502也可以包括非易失性存储器(Non-Volatile Memory,NVM),例如只读存储器(Read-Only Memory,ROM),快闪存储器(flash memory),硬盘(Hard Disk Drive,HDD)或固态硬盘(Solid-State Drive,SSD);存储器502还可以包括上述种类的存储器的组合。本发明实施例中,存储器502用于存储通信数据加密的程序、各种加密脚本、解密脚本、密钥等。

[0129] 所述通信接口503用于发送或接收数据。

[0130] 处理器501可以调用所述程序代码以执行以下操作:

[0131] 通过通信接口503获取终端设备发起的对目标页面的访问请求;

[0132] 通过通信接口503根据所述访问请求从所述目标页面对应的后台服务器获取所述目标页面对应的第一页面数据;

[0133] 采用第一加密算法对所述第一页面数据进行加密得到第二页面数据;

[0134] 通过通信接口503向所述终端设备发送对所述访问请求的第一响应,以使所述终端设备根据第一解密数据对所述第二页面数据进行解密得到所述第一页面数据,所述第一响应包括所述第二页面数据以及所述第一解密数据,所述第一解密数据为包含所述第一加密算法的数据。

[0135] 需要说明的是,各个操作的实现还可以对应参照图2-图3所示的方法实施例的相应描述;所述处理器501还可以与通信接口503配合执行上述方法实施例中的其他操作。

[0136] 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存储有计算机程序,所述计算机程序包括程序指令,所述程序指令当被计算机执行时使所述计算机执行如前述实施例所述的方法,所述计算机可以为上述提到的通信数据加密装置的一部分。例如为上述的处理器501。

[0137] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random Access Memory,RAM)等。

[0138] 以上所揭露的仅为本发明较佳实施例而已,当然不能以此来限定本发明之权利范围,因此依本发明权利要求所作的等同变化,仍属本发明所涵盖的范围。

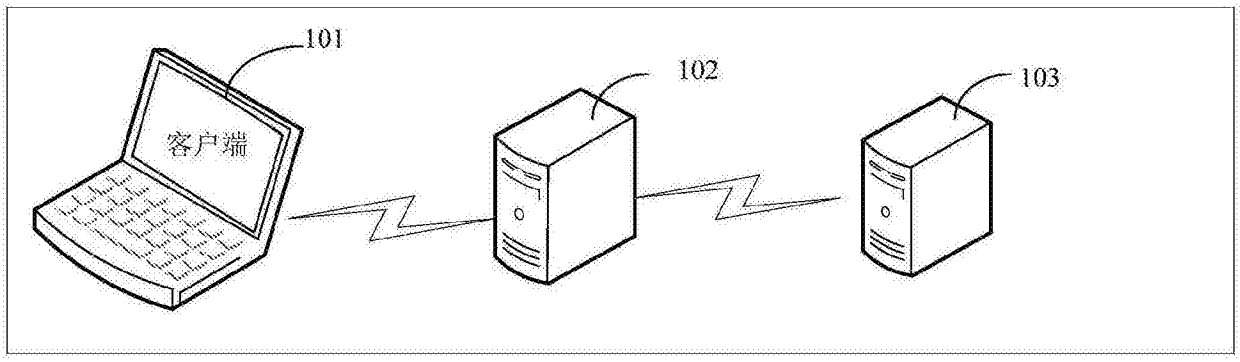

101
客户端
102
103

图1

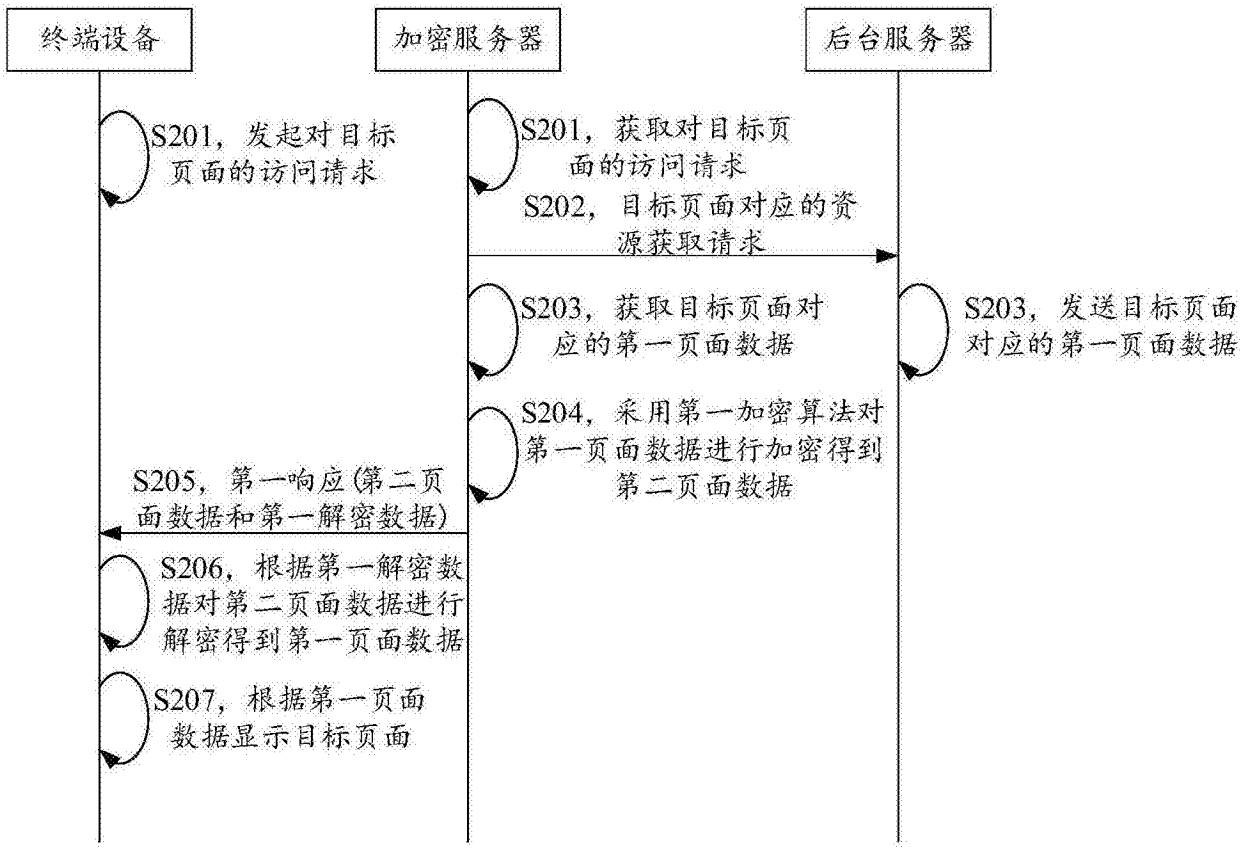

终端设备
加密服务器
后台服务器
S201，发起对目标页面的访问请求
S201，获取对目标页面的访问请求
S202，目标页面对应的资源获取请求
S203，获取目标页面对应的第一页面数据
S203，发送目标页面对应的第一页面数据
S204，采用第一加密算法对第一页面数据进行加密得到第二页面数据
S205，第一响应(第二页面数据和第一解密数据)
S206，根据第一解密数据对第二页面数据进行解密得到第一页面数据
S207，根据第一页面数据显示目标页面

图2

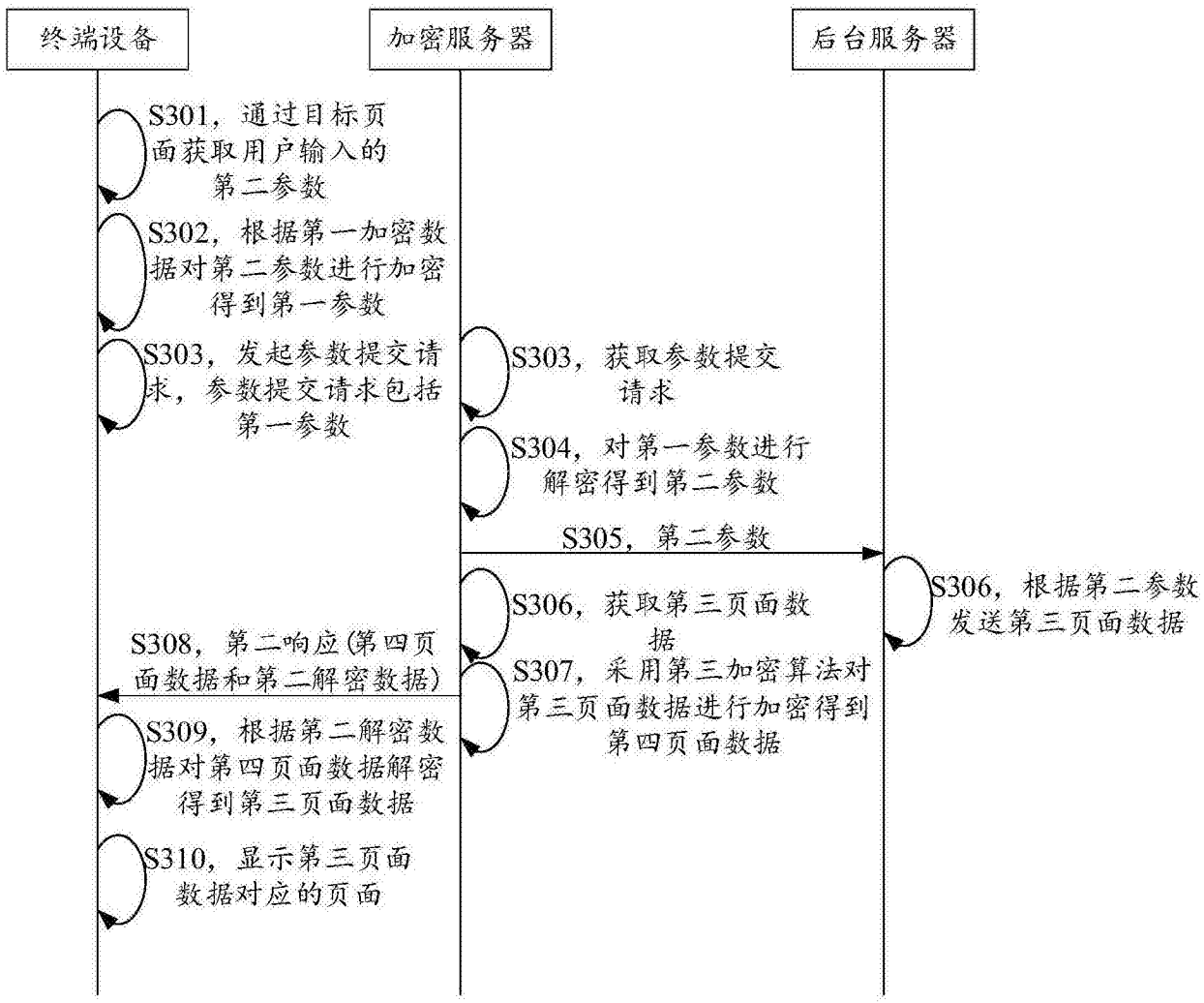

终端设备
加密服务器
后台服务器
S301，通过目标页面获取用户输入的第二参数
S302，根据第一加密数据对第二参数进行加密得到第一参数
S303，发起参数提交请求，参数提交请求包括第一参数
S303，获取参数提交请求
S304，对第一参数进行解密得到第二参数
S305，第二参数
S306，根据第二参数发送第三页面数据
S306，获取第三页面数据
S307，采用第三加密算法对第三页面数据进行加密得到第四页面数据
S308，第二响应(第四页面数据和第二解密数据)
S309，根据第二解密数据对第四页面数据解密得到第三页面数据
S310，显示第三页面数据对应的页面

图3

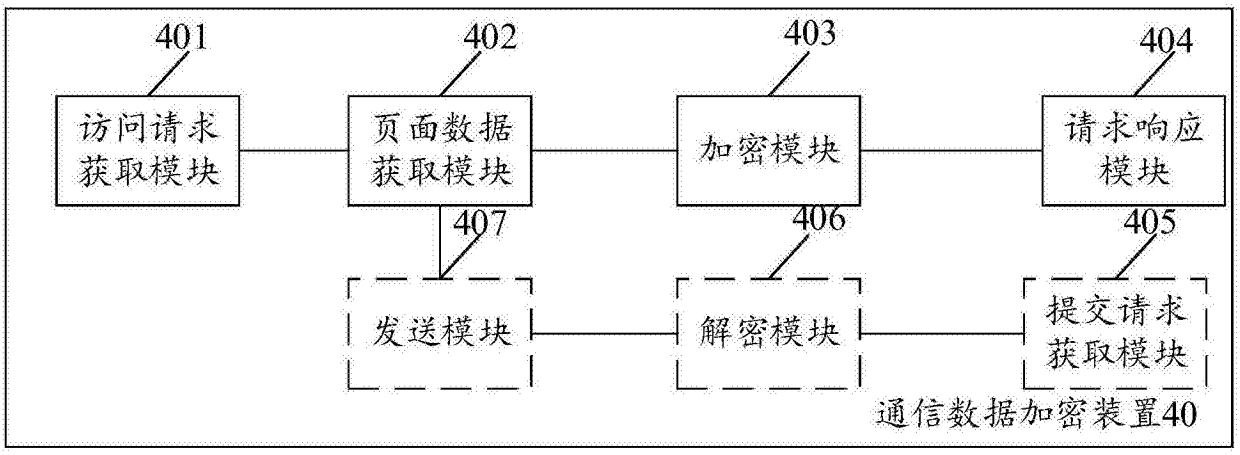

401
访问请求获取模块
402
页面数据获取模块
403
加密模块
404
请求响应模块
407
发送模块
406
解密模块
405
提交请求获取模块
通信数据加密装置40

图4

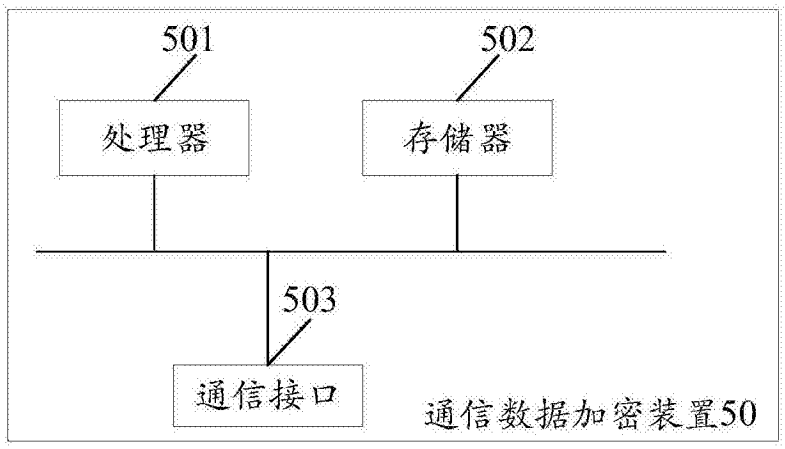


图5