(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 109005038 A
(43)申请公布日 2018.12.14

(21)申请号 201810878307.X

(22)申请日 2018.08.03

(71)申请人 北京达佳互联信息技术有限公司
地址 100084 北京市海淀区中关村东路1号院8号楼20层B2201

(72)发明人 刘硕

(74)专利代理机构 北京市立方律师事务所 11330
代理人 刘延喜

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/08(2006.01)

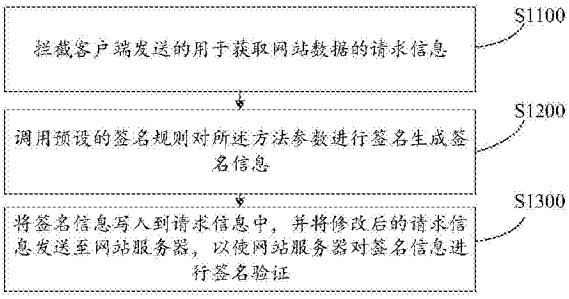
权利要求书2页 说明书9页 附图5页

(54)发明名称

签名方法、装置、电子设备及存储介质

(57)摘要

本公开提供了一种签名方法、装置、电子设备及存储介质，包括：拦截客户端发送的用于获取网站数据的请求信息，所述请求信息包括响应参数的可变的方法参数；调用预设的签名规则对所述方法参数进行签名生成签名信息；将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器，以使所述网站服务器对所述签名信息进行签名验证。利用拦截器拦截客户端发送的请求信息，并采用预设的签名规则对请求信息中方法参数进行签名，从而得到签名信息，该方法通过拦截器调用签名规则来进行签名，只需要将签名规则预存于客户端由客户端发送请求信息时包含在内即可，不需要客户端开发人员验证签名细节，方法简单。



CN 109005038 A

1.一种签名方法，应用于拦截器，其特征在于，包括：

拦截客户端发送的用于获取网站数据的请求信息，所述请求信息包括响应参数的可变的方法参数；

调用预设的签名规则对所述方法参数进行签名生成签名信息；

将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器，以使所述网站服务器对所述签名信息进行签名验证。

2.根据权利要求1所述的签名方法，其特征在于，所述请求信息包括超文本传输协议的名称；所述拦截客户端发送的用于获取网站数据的请求信息之前，包括：

获取所述请求信息中超文本传输协议的方法名称；

根据所述方法名称在预设的拦截器链中查找目标拦截器；

调用所述目标拦截器对所述请求信息进行拦截。

3.根据权利要求1所述的签名方法，其特征在于，所述签名规则包括：排序规则，所述调用预设的签名规则对所述方法参数进行签名生成签名信息，包括：

根据所述排序规则对所述方法参数进行排序生成第一字符串；

对所述第一字符串进行哈希运算生成签名信息。

4.根据权利要求1所述的签名方法，其特征在于，所述签名规则包括：排序规则，所述请求信息包括：身份信息和链接信息；所述调用预设的签名规则对所述方法参数进行签名生成签名信息，包括：

根据所述排序规则对所述方法参数进行排序生成第一字符串；

对所述第一字符串、身份信息和链接信息进行哈希运算生成签名信息。

5.根据权利要求4所述的签名方法，其特征在于，所述将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器，包括下述步骤：

获取预设的符号函数；

将所述签名信息带入到所述符号参数中生成报头字符；

将所述报头字符添加到所述请求信息的报头位置，并将写入所述报头字符的请求信息发送至网站服务器。

6.根据权利要求1所述的签名方法，其特征在于，当所述网站服务器验证所述签名信息合法时，所述将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器之后，包括：

接收所述网站服务器响应于所述请求信息发送的网站数据；

调用预设的解密算法对所述网站数据进行解密并发送至所述客户端。

7.根据权利要求1～6任一项所述的签名方法，其特征在于，所述签名规则包含于预先集成的归档文件数据包中。

8.一种签名装置，其特征在于，包括：

获取单元，被配置为执行拦截客户端发送的用于获取网站数据的请求信息，所述请求信息包括响应参数的可变的方法参数；

处理单元，被配置为执行调用预设的签名规则对所述方法参数进行签名生成签名信息；

执行单元，被配置为执行将所述签名信息写入到所述请求信息中，并将修改后的请求

信息发送至网站服务器，以使所述网站服务器对所述签名信息进行签名验证。

9.一种电子设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行如权利要求1至7中任一项权利要求所述签名方法的步骤。

10.一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种如权利要求1至7中任一项权利要求所述签名方法的步骤。

签名方法、装置、电子设备及存储介质

技术领域

[0001] 本公开涉及服务器领域，尤其涉及一种签名方法、装置、电子设备及存储介质。

背景技术

[0002] 目前的web服务中有很多应用程序接口(Application Program Interface,API)都采用了签名的方法进行参数以及请求的合法性验证。即，采用某些规则和密钥对数据进行签名后传递给服务器，服务器用相同的密钥计算出收到的数据的签名，并将计算出的签名与收到的签名进行比对，若相同则认为请求合法，继续执行业务并返回结果。

[0003] 相关的签名方法中需要在客户端开发签名代码，并设置具体的加密、解密算法，签名过程复杂、繁琐。

发明内容

[0004] 为克服相关技术中存在的问题，本公开提供一种签名方法。

[0005] 根据本公开实施例的第一方面，提供一种签名方法，包括：

[0006] 拦截客户端发送的用于获取网站数据的请求信息，所述请求信息包括响应参数的可变的方法参数；

[0007] 调用预设的签名规则对所述方法参数进行签名生成签名信息；

[0008] 将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器，以使所述网站服务器对所述签名信息进行签名验证。

[0009] 可选地，所述请求信息包括超文本传输协议的名称；所述拦截客户端发送的用于获取网站数据的请求信息之前，包括：

[0010] 获取所述请求信息中超文本传输协议的方法名称；

[0011] 根据所述方法名称在预设的拦截器链中查找目标拦截器；

[0012] 调用所述目标拦截器对所述请求信息进行拦截。

[0013] 可选地，所述签名规则包括：排序规则，所述调用预设的签名规则对所述方法参数进行签名生成签名信息，包括：

[0014] 根据所述排序规则对所述方法参数进行排序生成第一字符串；

[0015] 对所述第一字符串进行哈希运算生成签名信息。

[0016] 可选地，所述签名规则包括：排序规则，所述请求信息包括：身份信息和链接信息；所述调用预设的签名规则对所述方法参数进行签名生成签名信息，包括下述步骤：

[0017] 根据所述排序规则对所述方法参数进行排序生成第一字符串；

[0018] 对所述第一字符串、身份信息和链接信息进行哈希运算生成签名信息。

[0019] 可选地，所述将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器，包括：

[0020] 获取预设的符号函数；

[0021] 将所述签名信息带入到所述符号参数中生成报头字符；

[0022] 将所述报头字符添加到所述请求信息的报头位置，并将写入所述报头字符的请求信息发送至网站服务器。

[0023] 可选地，当所述网站服务器验证所述签名信息合法时，所述将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器之后，包括：

[0024] 接收所述网站服务器响应于所述请求信息发送的网站数据；

[0025] 调用预设的解密算法对所述网站数据进行解密并发送至所述客户端。

[0026] 可选地，所述签名规则包含于预先集成的归档文件数据包中。

[0027] 根据本公开实施例的第二方面，提供一种签名装置，包括：

[0028] 获取单元，被配置为执行拦截客户端发送的用于获取网站数据的请求信息，所述请求信息包括响应参数的可变的方法参数；

[0029] 处理单元，被配置为执行调用预设的签名规则对所述方法参数进行签名生成签名信息；

[0030] 执行单元，被配置为执行将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器，以使所述网站服务器对所述签名信息进行签名验证。

[0031] 可选地，所述请求信息包括超文本传输协议的名称；所述签名装置包括：

[0032] 方法获取单元，被配置为执行获取所述请求信息中超文本传输协议的方法名称；

[0033] 查找单元，被配置为执行根据所述方法名称在预设的拦截器链中查找目标拦截器；

[0034] 调用单元，被配置为执行调用所述目标拦截器对所述请求信息进行拦截。

[0035] 可选地，所述签名规则包括：排序规则，所述处理单元包括：

[0036] 第一生成单元，被配置为执行根据所述排序规则对所述方法参数进行排序生成第一字符串；

[0037] 第一计算单元，被配置为执行对所述第一字符串进行哈希运算生成签名信息。

[0038] 可选地，所述签名规则包括：排序规则，所述请求信息包括：身份信息和链接信息；所述处理单元包括：

[0039] 第二生成单元，被配置为执行根据所述排序规则对所述方法参数进行排序生成第一字符串；

[0040] 第二计算单元，被配置为执行对所述第一字符串、身份信息和链接信息进行哈希运算生成签名信息。

[0041] 可选地，所述执行单元包括：

[0042] 函数获取单元，被配置为执行获取预设的符号函数；

[0043] 报头生成单元，被配置为执行将所述签名信息带入到所述符号参数中生成报头字符；

[0044] 发送单元，被配置为执行将所述报头字符添加到所述请求信息的报头位置，并将写入所述报头字符的请求信息发送至网站服务器。

[0045] 可选地，当所述网站服务器验证所述签名信息合法时，所述签名装置还包括：

[0046] 接收单元，被配置为执行接收所述网站服务器响应于所述请求信息发送的网站数据；

[0047] 调用单元，被配置为执行调用预设的解密算法对所述网站数据进行解密并发送至

所述客户端。

[0048] 可选地，所述签名规则包含于预先集成的归档文件数据包中。

[0049] 根据本公开实施例的第三方面，提供一种电子设备，包括处理器；用于存储处理器可执行指令的存储器；其中，所述处理器被配置为执行如本公开第一方面提供的所述签名方法的步骤。

[0050] 根据本公开实施例的第四方面，提供一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行本公开第一方面提供的所述签名方法的步骤。

[0051] 根据本申请公开实施例的第五方面，提供一种计算机程序产品，包括计算机程序代码，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述签名方法的步骤。

[0052] 本公开的实施例提供的技术方案可以包括以下有益效果：利用拦截器拦截客户端发送的请求信息，并采用预设的签名规则对请求信息中方法参数进行签名，从而得到签名信息，该方法通过拦截器调用签名规则来进行签名，只需要将签名规则预存于客户端由客户端发送请求信息时包含在内即可，不需要客户端开发人员验证签名细节，方法简单。

[0053] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

[0054] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施例，并与说明书一起用于解释本发明的原理。

[0055] 图1是根据一示例性实施例示出的一种签名方法的基本流程示意图；

[0056] 图2是根据一示例性实施例示出的目标拦截器的选取方法的基本流程示意图；

[0057] 图3是根据一示例性实施例示出的对方法参数进行签名的方法的基本流程示意图；

[0058] 图4是根据一示例性实施例示出的对方法参数进行签名生成签名信息方法的基本流程示意图；

[0059] 图5根据一示例性实施例示出的将签名信息写入到请求信息方法的基本流程示意图；

[0060] 图6是根据一示例性实施例示出的发送网站数据方法的基本流程示意图；

[0061] 图7是根据一示例性实施例示出的一种签名装置的框图；

[0062] 图8为根据一示例性实施例示出的一种移动终端的框图；

[0063] 图9是根据一示例性实施例示出的电子设备的框图。

具体实施方式

[0064] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和签名方法的例子。

[0065] 请参阅图1,图1是根据一示例性实施例示出的一种签名方法的基本流程示意图。

[0066] 如图1所示,签名方法包括下述步骤:

[0067] S1100、拦截客户端发送的用于获取网站数据的请求信息;

[0068] 本发明实施例中的签名方法应用于拦截器,即拦截器对客户端发送的请求信息进行拦截,并对请求信息进行签名,从而生成签名信息。其中,拦截器可以设置于客户端、服务器中,用于在某个方法或者字段被访问执行前进行拦截,然后再之前或之后加入某些操作,以实现具体功能,例如,要实现不能访问X网站的功能时,拦截器在接收到客户端访问X网站的请求后,对访问请求进行拦截,客户端不显示X网站。

[0069] 请求信息为客户端发送的用于获取网站数据的请求的信息,包括响应参数的可变的方法参数。其中,响应参数用于当服务器接收到客户端发送的请求信息后控制服务器对请求信息进行响应的参数,其中,响应参数包括多个可变的方法参数params,params是一个计算机函数,表示函数的参数时可变个数的,即表示类型相同,参数数量不确定。

[0070] S1200、调用预设的签名规则对所述方法参数进行签名生成签名信息;

[0071] 签名规则为拦截器用来对可变的方法参数进行签名的规则。其中,签名规则包含于预先集成的归档文件(Java Archive,jar)数据包中。其中,jar数据包是与平台无关的文件格式,允许将许多文件组合成一个压缩文件,jar文件可以用于部署和封装库、组件和插件程序,可被像编译器和JVM的工具直接使用。jar文件可以作为应用程序和扩展的构建单元、以及作为组件、applet或者插件程序使用。本发明实施例中,将签名规则及响应参数封装于jar文件中,并将jar文件集成于客户端登录的网站,如此,在对客户端发送的请求信息进行签名时,可以减少客户端开发人员的工作量。

[0072] 拦截器通过从jar数据包中调用签名规则,并利用签名规则对方法参数进行签名,生成签名信息。其中,签名规则可以按照实际情况进行设置,在此不作限定。

[0073] S1300、将签名信息写入到请求信息中,并将修改后的请求信息发送至网站服务器,以使网站服务器对签名信息进行签名验证。

[0074] 签名信息为对请求信息中包含的方法参数按照预设的方法进行密码变换或者添加字符后的信息。常用的签名算法包括:RSA、EIGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir数字签名算法、Des/DSA,椭圆曲线数字签名算法和有限自动机数字签名算法等。在实际应用中为保护传输中数据的私密性和完整性,防止被伪造,可以按照实际情况对签名算法进行设置。

[0075] 拦截器将签名后的字符写入到请求信息的报头中,并发送至网站服务器,使网站服务器对签名信息进行签名验证。

[0076] 本发明实施例的签名方法,利用拦截器拦截客户端发送的请求信息,并采用预设的签名规则对请求信息中方法参数进行签名,从而得到签名信息,该方法通过拦截器调用签名规则来进行签名,只需要将签名规则预存于客户端由客户端发送请求信息时包含在内即可,不需要客户端开发人员验证签名细节,方法简单。

[0077] 实际应用中,拦截器可以设置于客户端或者服务器,本实施例中,拦截器设置于拦截服务器中,客户端发送的请求信息中包含了超文本传输协议(HyperText Transfer Protocol,HTTP),因此,拦截器拦截客户端发送的请求信息之前,需要对应HTTP的方法名称选取对应的拦截器。请参阅图2,图2是根据一示例性实施例示出的目标拦截器的选取方法

的基本流程示意图。

[0078] 如图2所示，步骤S1100之前，包括：

[0079] S1111、获取请求信息中超文本传输协议的方法名称；

[0080] 当拦截服务器接收到客户端发送的请求信息的数据包后，在数据包的包头获取HTTP的方法名称。

[0081] S1112、根据方法名称在预设的拦截器链中查找目标拦截器；

[0082] S1113、调用目标拦截器对请求信息进行拦截。

[0083] 实际应用中，拦截服务器通常为代理服务器，代理服务器中预设有拦截器链，即多个拦截器，每个拦截器针对一种网络传输协议的数据，因此，代理服务器根据HTTP的方法名称在拦截器链中查找适用于HTTP的目标拦截器，以对请求信息进行拦截。

[0084] 需要说明的是，网络传输协议是计算机通信的传送协议，例如有传输控制协议(Transmission Control Protocol，TCP)、网络控制协议(Network Control Protocol，NCP)网络新闻传输协议(NNTP，Network News Transfer Protocol)等。

[0085] 本发明的一个实施例，签名规则包括排序规则，请参阅图3，图3是根据一示例性实施例示出的对方法参数进行签名的方法的基本流程示意图。

[0086] 如图3所示，步骤S1200包括：

[0087] S1211、根据排序规则对方法参数进行排序生成第一字符串；

[0088] 其中排序规则为对可变的方法参数进行排序的规则，可以为从大到小的顺序，也可以为从小到大的顺序，具体不作限定，利用排序规则对可变的方法参数进行排序可以确保可变的方法参数按照确定的顺序排列以使签名后的可变方法参数的第一字符串为唯一确定的。

[0089] S1212、对第一字符串进行哈希运算生成签名信息。

[0090] 代理服务器对第一字符串进行哈希运算，生成签名信息，本实施例中，哈希运算可以为hmacsha256算法，

[0091] 本发明的一个实施例，签名规则包括：排序规则，客户端发送的请求信息包括：身份信息和链接信息；请参阅图4，图4是根据一示例性实施例示出的对方法参数进行签名生成签名信息方法的基本流程示意图。

[0092] 如图4所示，步骤S1200包括：

[0093] S1221、根据排序规则对方法参数进行排序生成第一字符串；

[0094] 本实施例中生成第一字符串的具体方法请参阅图3所示的实施例，在此不再赘述。

[0095] S1222、对第一字符串、身份信息和链接信息进行哈希运算生成签名信息。

[0096] 身份信息为表示客户端发送请求信息中所携带的用户的信息，例如，用户通过合法途径在XX网站注册了账户信息，则用户通过客户端发送请求时，请求中会携带用户账户的信息。通常，采用储存在用户本地终端上的数据cookie，即为辨别用户身份进行session跟踪而储存在用户本地终端上的数据。

[0097] 链接信息为表示网络传输协议链接的信息，例如HTTP Header，通过网址输入，可以分析页面的HTTP头信息或者显示。

[0098] 本发明的一个实施例，请参阅图5，图5根据一示例性实施例示出的将签名信息写入到请求信息方法的基本流程示意图。

[0099] 如图5所示，步骤S1300包括：

[0100] S1311、获取预设的符号函数；

[0101] 报文是网络中交换与传输的数据单元，即站点一次性要发送的数据块，报文在传输过程中会不断的封装成分组、包、帧来进行传输，封装的方式就是添加一些信息段，即报头以一定格式组织起来的数据。通常情况下，报文在封装过程中通过采用一些加密算法将原数据转化为特定的符号。

[0102] 本公开实施例中涉及的预设的符号函数即为上述加密算法，例如，普通数字签名和特殊数字签名。普通数字签名算法有RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir数字签名算法、Des/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，上述签名方式可以按照具体应用环境进行选择。

[0103] S1312、将签名信息带入到符号参数中生成报头字符；

[0104] 本实施例中利用上述符号函数，即加密函数对生成的签名信息转换为字符。

[0105] S1313、将报头字符添加到请求信息的报头位置，并将写入报头字符的请求信息发送至网站服务器。

[0106] 本实施例中，将生成的字符添加到请求信息的报头的标志位中，以及将写入的请求信息发送至网站服务器。

[0107] 当网站服务器验证签名信息合法时，请参阅图6，图6是根据一示例性实施例示出的发送网站数据方法的基本流程示意图。

[0108] 如图6所示，步骤S1300之后包括：

[0109] S1321、接收网站服务器响应于请求信息发送的网站数据；

[0110] 需要说明的是，网站服务器中预存有与拦截器所使用的签名规则相同的签名规则，如此，当网站服务器接收到修改后的请求信息后，从请求信息中获取响应参数的可变的方法参数，利用相同的排序规则对可变的方法参数进行排序得到第一字符串，以及对第一字符串进行哈希运算得到签名信息。或者，将第一字符串与身份信息、链接信息进行哈希运算得到签名信息。网站服务器将自身得到的签名信息与接收代理服务器发送的签名信息进行比对，当二者相同时，则确定签名合法，当二者不同时，则确定签名不合法。当签名合法时，网站服务器对请求信息进行响应，利用预设的加密方法对网站数据进行加密，并发送给拦截器所在的代理服务器。

[0111] 拦截器所在的代理服务器接收网站服务器发送的网站数据。

[0112] S1322、调用预设的解密算法对网站数据进行解密并发送至客户端。

[0113] 拦截器所在的代理服务器利用预设的解密算法对网站数据进行解密。实际应用中，预设的解密算法包含于预先集成的jar数据包中。其中，解密算法与网站服务器中对网站数据加密的算法相对应。本发明的另一个实施例，当签名不合法时，拦截器所在的代理服务器发送提示信息给客户端，提示用户网站数据不可显示。

[0114] 为解决上述技术问题本发明实施例还提供一种签名装置。具体请参阅图7，图7是根据一示例性实施例示出的一种签名装置的框图。

[0115] 如图7所示，一种签名装置，包括：获取模块2100、处理模块2200和执行模块2300。

其中，获取单元，被配置为执行拦截客户端发送的用于获取网站数据的请求信息，所述请求信息包括响应参数的可变的方法参数；处理单元，被配置为执行调用预设的签名规则对所述方法参数进行签名生成签名信息；执行单元，被配置为执行将所述签名信息写入到所述请求信息中，并将修改后的请求信息发送至网站服务器，以使所述网站服务器对所述签名信息进行签名验证。

[0116] 本公开的实施例提供的技术方案可以包括以下有益效果：利用拦截器拦截客户端发送的请求信息，并采用预设的签名规则对请求信息中方法参数进行签名，从而得到签名信息，该方法通过拦截器调用签名规则来进行签名，只需要将签名规则预存于客户端由客户端发送请求信息时包含在内即可，不需要客户端开发人员验证签名细节，方法简单。

[0117] 在一些实施方式中，所述请求信息包括超文本传输协议的方法名称；所述签名装置包括：方法获取单元，被配置为执行获取所述请求信息中超文本传输协议的方法名称；查找单元，被配置为执行根据所述方法名称在预设的拦截器链中查找目标拦截器；调用单元，被配置为执行调用所述目标拦截器对所述请求信息进行拦截。

[0118] 在一些实施方式中，所述签名规则包括：排序规则，所述处理单元包括：第一生成单元，被配置为执行根据所述排序规则对所述方法参数进行排序生成第一字符串；第一计算单元，被配置为执行对所述第一字符串进行哈希运算生成签名信息。

[0119] 在一些实施方式中，所述签名规则包括：排序规则，所述请求信息包括：身份信息和链接信息；所述处理单元包括：第二生成单元，被配置为执行根据所述排序规则对所述方法参数进行排序生成第一字符串；第二计算单元，被配置为执行对所述第一字符串、身份信息和链接信息进行哈希运算生成签名信息。

[0120] 在一些实施方式中，所述执行单元包括：函数获取单元，被配置为执行获取预设的符号函数；报头生成单元，被配置为执行将所述签名信息带入到所述符号参数中生成报头字符；发送单元，被配置为执行将所述报头字符添加到所述请求信息的报头位置，并将写入所述报头字符的请求信息发送至网站服务器。

[0121] 在一些实施方式中，当所述网站服务器验证所述签名信息合法时，所述签名装置还包括：接收单元，被配置为执行接收所述网站服务器响应于所述请求信息发送的网站数据；调用单元，被配置为执行调用预设的解密算法对所述网站数据进行解密并发送至所述客户端。

[0122] 在一些实施方式中，所述签名规则包含于预先集成的归档文件数据包中。

[0123] 图8是根据一示例性实施例示出的一种用于签名的移动终端700的框图。例如，移动终端700可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

[0124] 参照图8，移动终端700可以包括以下一个或多个组件：处理组件702，存储器704，电力组件706，多媒体组件708，音频组件710，输入/输出(I/O)的接口712，传感器组件714，以及通信组件716。

[0125] 处理组件702通常控制移动终端700的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理组件702可以包括一个或多个处理器720来执行指令，以完成上述的签名方法的全部或部分步骤。此外，处理组件702可以包括一个或多个模块，便于处理组件702和其他组件之间的交互。例如，处理组件702可以包括多媒体模

块，以方便多媒体组件708和处理组件702之间的交互。

[0126] 存储器704被配置为存储各种类型的数据以支持在移动终端700的操作。这些数据的示例包括用于在移动终端700上操作的任何应用程序或路由数据处理方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器704可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(SRAM)，电可擦除可编程只读存储器(EEPROM)，可擦除可编程只读存储器(EPROM)，可编程只读存储器(PROM)，只读存储器(ROM)，磁存储器，快闪存储器，磁盘或光盘。

[0127] 电源组件706为移动终端700的各种组件提供电力。电源组件706可以包括电源管理系统，一个或多个电源，及其他与为移动终端700生成、管理和分配电力相关联的组件。

[0128] 多媒体组件708包括在所述移动终端700和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器(LCD)和触摸面板(TP)。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件708包括一个前置摄像头和/或后置摄像头。当设备700处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0129] 音频组件710被配置为输出和/或输入音频信号。例如，音频组件710包括一个麦克风(MIC)，当移动终端700处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器704或经由通信组件716发送。在一些实施例中，音频组件710还包括一个扬声器，用于输出音频信号。

[0130] I/O接口712为处理组件702和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

[0131] 传感器组件714包括一个或多个传感器，用于为移动终端700提供各个方面的状态评估。例如，传感器组件714可以检测到设备700的打开/关闭状态，组件的相对定位，例如所述组件为移动终端700的显示器和小键盘，传感器组件714还可以检测移动终端700或移动终端700一个组件的位置改变，用户与移动终端700接触的存在或不存在，移动终端700方位或加速/减速和移动终端700的温度变化。传感器组件714可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件714还可以包括光传感器，如CMOS或CCD图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件714还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

[0132] 通信组件716被配置为便于移动终端700和其他设备之间有线或无线方式的通信。移动终端700可以接入基于通信标准的无线网络，如WiFi，运营商网络(如2G、3G、4G或5G)，或它们的组合。在一个示例性实施例中，通信组件716经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件716还包括近场通信(NFC)模块，以促进短程通信。例如，在NFC模块可基于射频识别(RFID)技术，红外数据协会(IrDA)技术，超宽带(UWB)技术，蓝牙(BT)技术和其他技术来实现。

[0133] 在示例性实施例中，移动终端700可以被一个或多个应用专用集成电路(ASIC)、数

字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述签名方法。

[0134] 在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器704，上述指令可由移动终端700的处理器720执行以完成上述路由数据处理方法。例如，所述非临时性计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0135] 图8是根据一示例性实施例示出的一种用于签名的电子设备800的框图。例如，电子设备800可以被提供为一服务器。参照图8，电子设备800包括处理组件822，其进一步包括一个或多个处理器，以及由存储器832所代表的存储器资源，用于存储可由处理组件822的执行的指令，例如应用程序。存储器832中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理组件822被配置为执行指令，以执行上述签名方法。

[0136] 电子设备800还可以包括一个电源组件826被配置为执行电子设备800的电源管理，一个有线或无线网络接口850被配置为将电子设备800连接到网络，和一个输入输出(I/O)接口858。电子设备800可以操作基于存储在存储器832的操作系统，例如Windows ServerTM,Mac OS XTM,UnixTM,LinuxTM,FreeBSDTM或类似。

[0137] 一种计算机程序产品，包括计算机程序代码，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行上述签名方法。

[0138] 本领域技术人员在考虑说明书及实践这里公开后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

[0139] 应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

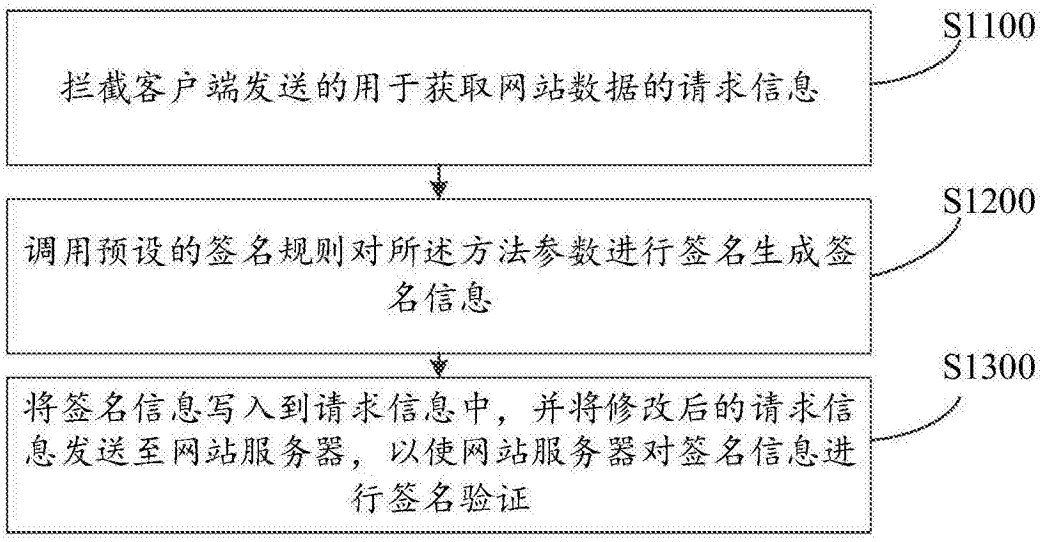

S1100
拦截客户端发送的用于获取网站数据的请求信息
S1200
调用预设的签名规则对所述方法参数进行签名生成签名信息
S1300
将签名信息写入到请求信息中，并将修改后的请求信息发送至网站服务器，以使网站服务器对签名信息进行签名验证

图1

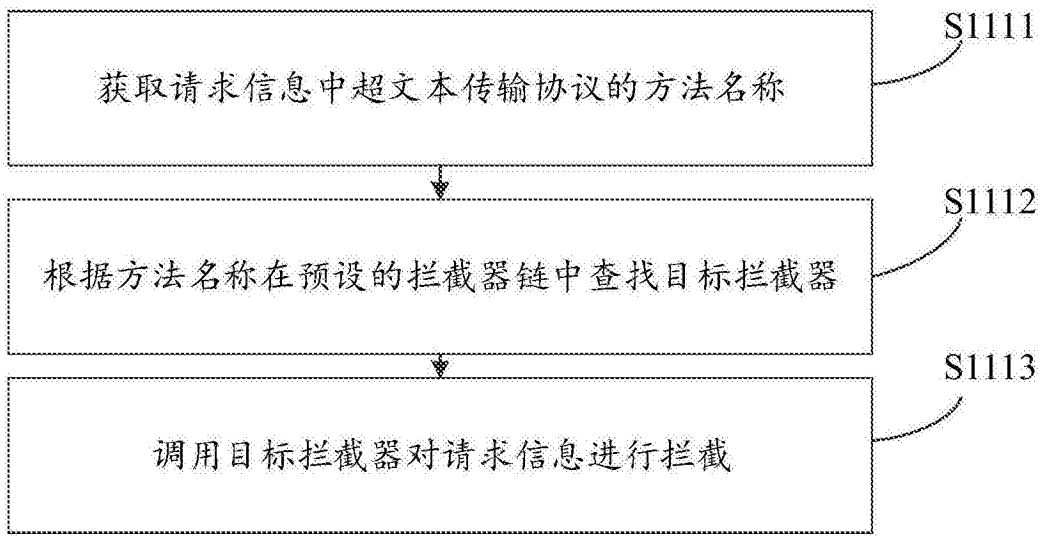

S1111
获取请求信息中超文本传输协议的方法名称
S1112
根据方法名称在预设的拦截器链中查找目标拦截器
S1113
调用目标拦截器对请求信息进行拦截

图2

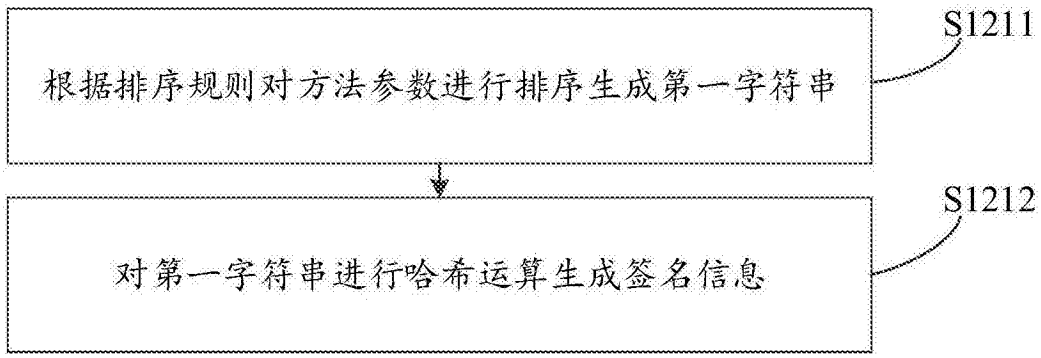

S1211
根据排序规则对方法参数进行排序生成第一字符串
S1212
对第一字符串进行哈希运算生成签名信息

图3

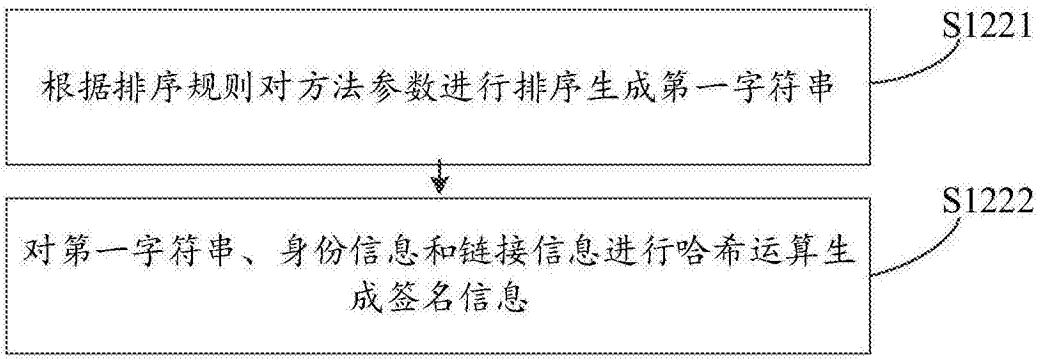

S1221
根据排序规则对方法参数进行排序生成第一字符串
S1222
对第一字符串、身份信息和链接信息进行哈希运算生成签名信息

图4

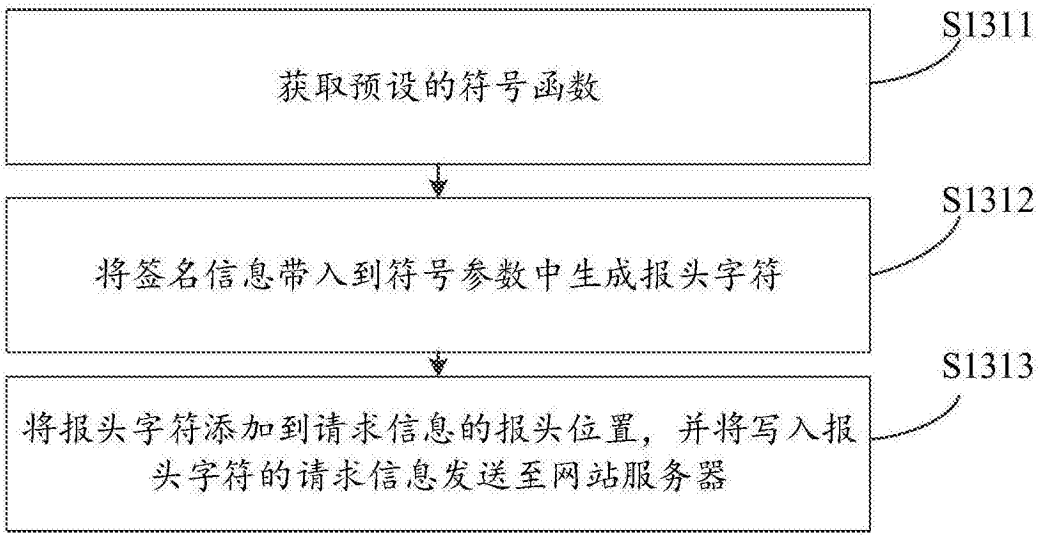

S1311
获取预设的符号函数
S1312
将签名信息带入到符号参数中生成报头字符
S1313
将报头字符添加到请求信息的报头位置，并将写入报头字符的请求信息发送至网站服务器

图5

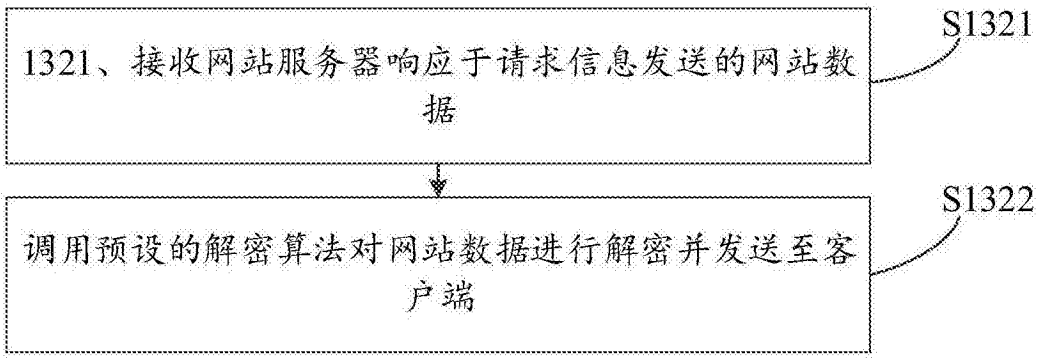

S1321
1321、接收网站服务器响应于请求信息发送的网站数据
S1322
调用预设的解密算法对网站数据进行解密并发送至客户端

图6

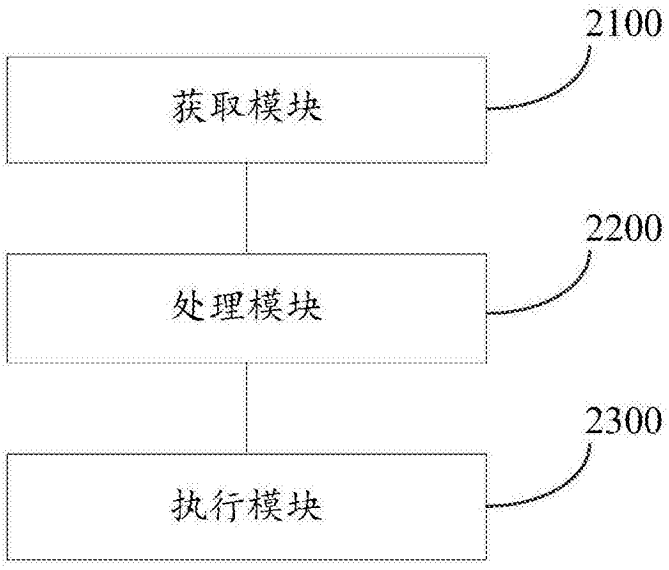


图7

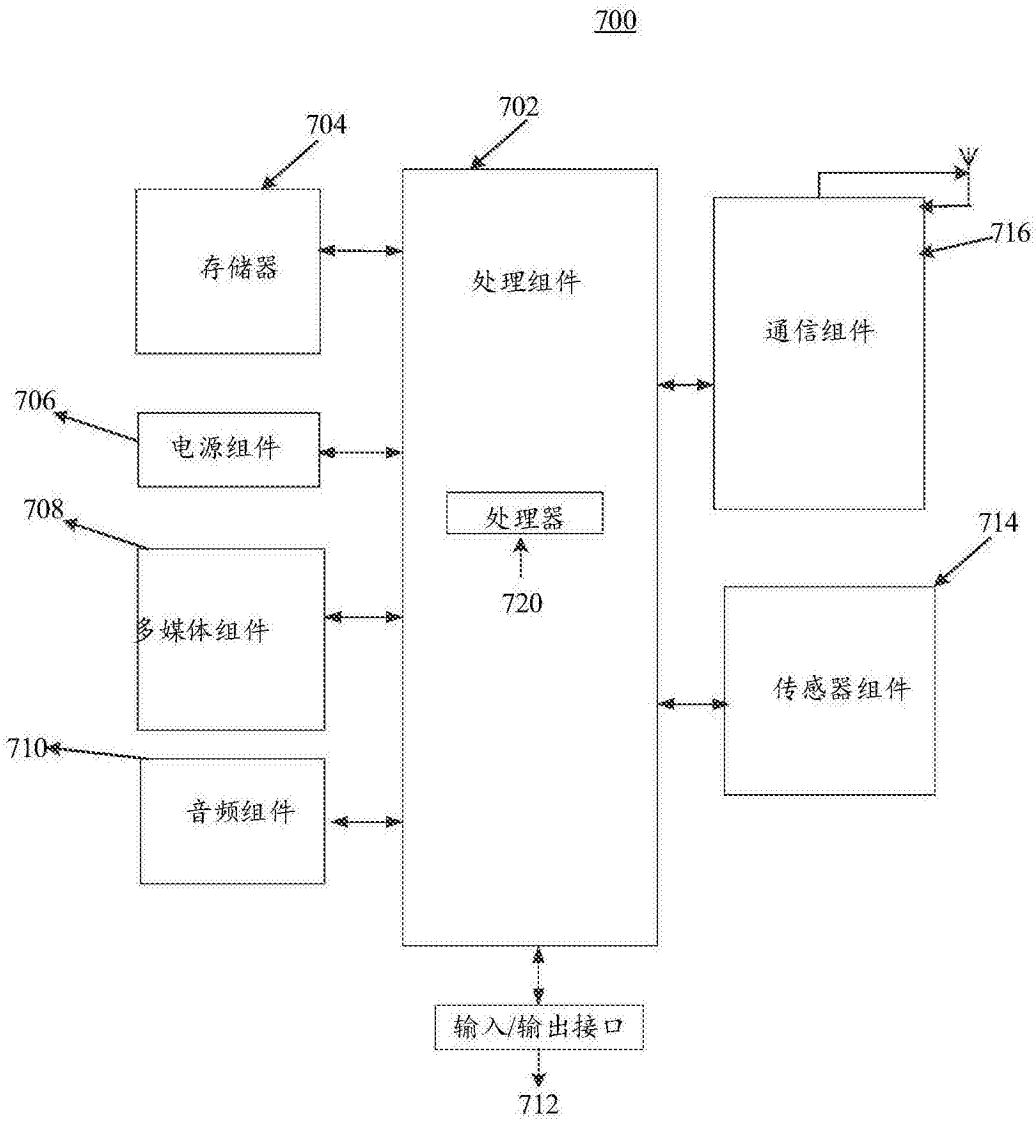

700
704
702
存储器
处理组件
716
通信组件
706
电源组件
处理器
720
708
多媒体组件
714
传感器组件
710
音频组件
输入/输出接口
712

图8

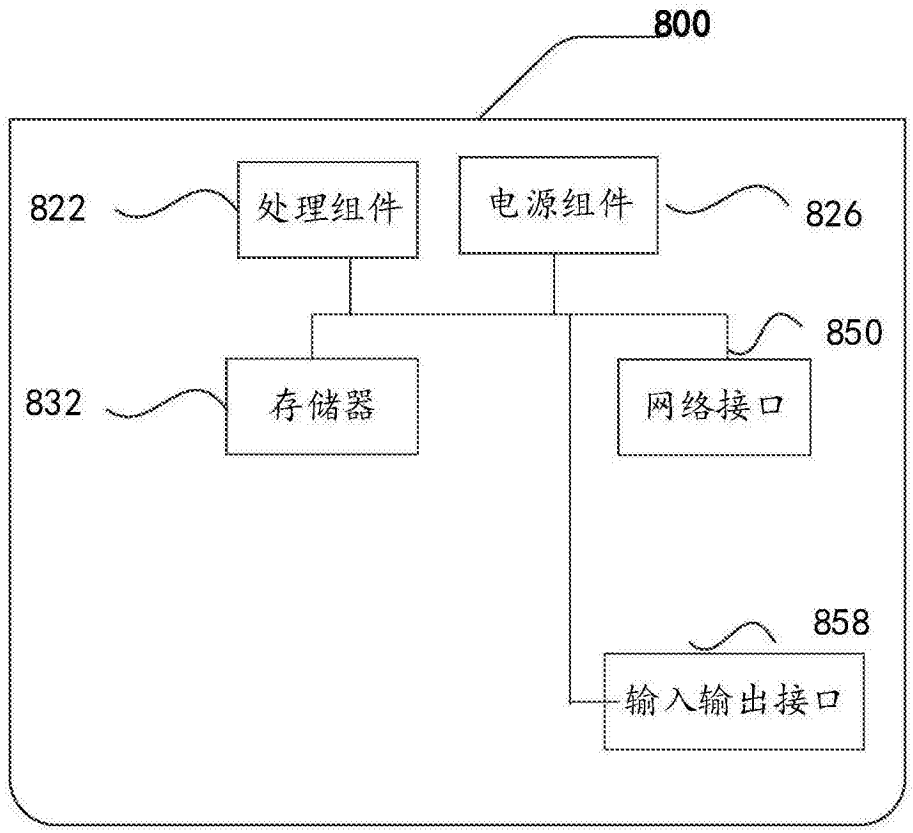


图9