



(12) 发明专利申请

(10) 申请公布号 CN 105208024 A

(43) 申请公布日 2015. 12. 30

(21) 申请号 201510606961. 1

(22) 申请日 2015. 09. 22

(71) 申请人 深圳市金溢科技股份有限公司

地址 518057 广东省深圳市南山区科苑路清
华信息港研发楼 A 栋 12 层

(72) 发明人 何小川 段作义 杨耿

(74) 专利代理机构 深圳鼎合诚知识产权代理有
限公司 44281

代理人 林宏津 陈俊斌

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 9/32(2006. 01)

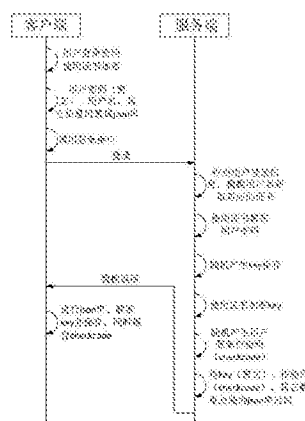
权利要求书2页 说明书8页 附图7页

(54) 发明名称

不使用 HTTPS 的数据安全传输方法及系统、
客户端和服务端

(57) 摘要

本申请涉及不使用 HTTPS 的数据安全传输方法及系统、客户端和服务端。方法包括：服务端在本地创建 CA，并向相连的客户端颁发用户证书，用户证书用作客户端登录服务端的登录凭证；服务端在收到客户端的登录信息后，根据登录凭证分配密钥，并将密钥返回给客户端；服务端根据密钥加密或解密客户端发来的数据信息。本申请通过服务端自己创建 CA，所有用户证书由该 CA 颁发，不需要额外付费购买第三方 CA；服务端在收到登录信息后，分配密钥给客户端，这样客户端可以使用该密钥对数据信息加密（解密）操作，而服务端可以使用该密钥对客户端发送来的数据信息进行解密（加密）操作，从而，在不使用 HTTPS 协议进行传输时，也能安全传输数据，实现了数据传输的双向认证。



1. 一种不使用基于安全套接字层的超文本传输协议的数据安全传输方法,用于车辆卡管理系统,其特征在于,包括以下步骤:

注册步骤:服务端在本地创建证书授权中心,并向相连的客户端颁发用户证书,所述用户证书用作所述客户端登录所述服务端的登录凭证;

登录步骤:所述服务端在收到所述客户端的登录信息后,根据所述登录凭证分配密钥,并将所述密钥返回给所述客户端;

加解密步骤:所述服务端根据所述密钥加密或解密所述客户端发来的数据信息。

2. 如权利要求 1 所述的方法,其特征在于,所述注册步骤具体包括:

所述服务端自己创建所述证书授权中心,并在接收到所述客户端的注册信息时,向所述客户端颁发所述证书授权中心认证的用户证书,并保存所述客户端相关的信息及其对应的用户证书,所述客户端相关的信息至少包括所述客户端的用户名和密码。

3. 如权利要求 2 所述的方法,其特征在于,所述登录步骤具体包括:

所述服务端接收所述客户端发送来的登录信息,所述登录信息包括所述客户端的用户名和已被加密的密码,所述密码使用所述用户证书加密;

所述服务端根据所述用户名取得对应的用户证书,使用所述用户证书解密所述已被加密的密码,随机产生密钥,并保存所述密钥;

所述服务端将所述密钥返回给所述客户端。

4. 如权利要求 1 所述的方法,其特征在于,

所述登录步骤还包括生成识别步骤,在所述生成识别步骤中,所述服务端根据所述登录凭证生成用户识别码,并将所述用户识别码返回给所述客户端,所述用户识别码被用作所述客户端在当前与所述服务端连接中的身份标识,并被用于在所述客户端发送数据信息时加入所述数据信息;

所述加解密步骤还包括用户识别步骤,在所述用户识别步骤中,所述服务端在接收到所述客户端发送的数据信息后,解析所述数据信息得到用户识别码,根据所述用户识别码确定所述数据信息对应的客户端,并响应所述对应的客户端。

5. 如权利要求 4 所述的方法,其特征在于,

所述生成识别步骤具体包括:所述服务端在接收到所述客户端发送来的登录信息后,根据所述客户端的登录凭证随机产生用户识别码,保存所述用户识别码,并将所述用户识别码返回给所述客户端;

所述用户识别步骤中,所述服务端在确定出所述数据信息对应的客户端后,获得所述对应的客户端的密钥。

6. 如权利要求 1 所述的方法,其特征在于,还包括接口定制步骤:

所述服务端根据所述客户端的类型和业务功能提供安全接口信息,并向所述客户端公布所述安全接口信息,所述安全接口信息用于指示需要加解密操作的接口;

所述服务端根据所述客户端发送来的携带有与安全接口信息相关内容的的数据信息,结合所述安全接口信息确定关于待传输数据的加解密操作。

7. 如权利要求 6 所述的方法,其特征在于,

所述安全接口信息包括安全接口列表,所述安全接口列表中登记有需要对传输数据进行加解密操作的接口;或者,所述安全接口信息包括带有安全参数值的接口函数,所述安全

参数值用于表征接口安全的级别。

8. 一种使用如权利要求 1-7 任一项所述的方法实现的不使用基于安全套接字层的超文本传输协议的数据安全传输系统,所述数据安全传输系统用于车辆卡管理系统。

9. 一种用于如权利要求 1-7 任一项所述的方法的客户端。

10. 一种用于如权利要求 1-7 任一项所述的方法的服务端。

不使用 HTTPS 的数据安全传输方法及系统、客户端和服务端

技术领域

[0001] 本申请涉及广域物联网组网技术领域,具体涉及一种数据安全传输方法和系统、及其涉及的客户端和服务端。

背景技术

[0002] 物联网是指按约定的协议,把物品与互联网连接起来,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的一种网络。物联网的典型应用之一是车辆管理系统,尤其是针对车辆卡(包括基于电子标签的 IC 卡)的管理系统。目前,车辆卡管理系统使用传统的三层架构方案,由数据访问层、业务逻辑层、表示层组成,如图 1 所示。业务逻辑层使用 Webserver 建立后台服务器,表示层通过访问 Webserver 提供的接口实现业务逻辑数据传输。

[0003] 在车辆卡管理系统中,终端客户的种类不唯一,不同业务对数据保密级别的要求也不一样,一些特殊的数据需要进行加密传输,传统的处理方法是使用 HTTPS 协议(Hyper Text Transfer Protocol over Secure Socket Layer,基于安全套接字层的超文本传输协议)来进行数据的安全传输控制。对于车辆卡系统,使用 HTTPS 协议存在以下的不足:

[0004] 1、服务器必须从 CA(Certificate Authority,证书授权中心)申请一个用于证明服务器用途类型的证书,免费证书很少,通常需要交费;

[0005] 2、HTTPS 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议,认证过程复杂,单次认证过程比较漫长,一般用于银行、交易支付方面;

[0006] 3、使用 HTTPS 协议的服务端和客户端之间的所有通讯都是加密的,无法定制加密数据段,如果需要定制加密接口,则需要使用两套协议方案,一套使用 HTTPS 传输协议,一套使用 HTTP 传输协议,不便于维护。

发明内容

[0007] 本申请提供一种适用于车辆卡管理系统的数据安全传输方法及系统,该方法和系统也可以适用于广域物联网的其他应用。

[0008] 根据本申请的第一方面,本申请提供一种不使用基于安全套接字层的超文本传输协议(HTTPS)的数据安全传输方法,该方法包括以下步骤:

[0009] 注册步骤:服务端在本地创建证书授权中心(CA),并向相连的客户端颁发用户证书,所述用户证书用作所述客户端登录所述服务端的登录凭证;

[0010] 登录步骤:所述服务端在收到所述客户端的登录信息后,根据所述登录凭证分配密钥,并将所述密钥返回给所述客户端;

[0011] 加解密步骤:所述服务端根据所述密钥加密或解密所述客户端发来的数据信息。

[0012] 进一步地,该方法的所述登录步骤还包括生成识别步骤,在所述生成识别子步骤中,所述服务端根据所述登录凭证生成用户识别码,并将所述用户识别码返回给所述客户

端 ;所述加解密步骤还包括用户识别步骤,在所述用户识别步骤中,所述服务端在接收到所述客户端发送的数据信息后,根据所述用户识别码确定所述数据信息对应的客户端,并响应所述对应的客户端。

[0013] 进一步地,该方法还包括接口定制步骤:所述服务端根据所述客户端的类型和业务功能提供安全接口信息,并向所述客户端公布所述安全接口信息,所述安全接口信息用于指示需要加解密操作的接口;所述服务端根据所述客户端发送来的携带有与安全接口信息相关内容的的数据信息,结合所述安全接口信息确定关于待传输数据的加解密操作。

[0014] 进一步地,在该方法中,传输于所述服务端和所述客户端之间的数据的格式为 JSON 数据交换格式;和/或,所述服务端和所述客户端之间的加密数据使用 BASE64 进行编码后再传输。

[0015] 根据本申请的第二方面,本申请提供一种使用如上所述方法实现的不使用 HTTPS 的数据安全传输系统。

[0016] 根据本申请的第三方面,本申请提供一种用于如上所述方法的客户端。

[0017] 根据本申请的第四方面,本申请提供一种用于如上所述方法的服务端。

[0018] 本申请的有益效果是:通过服务端自己创建 CA,所有用户证书由该 CA 颁发,不需要额外付费购买第三方的 CA;服务端在收到登录信息后,分配密钥给客户端,这样客户端可以使用该密钥对数据信息加密(解密)操作,而服务端可以使用该密钥对客户端发送来的数据信息进行解密(加密)操作,从而,在不使用 HTTPS 协议进行传输时,也能安全传输数据,实现了数据传输的双向认证。

附图说明

[0019] 图 1 为车辆卡管理系统的三层架构方案示意图;

[0020] 图 2 示出了本申请一种实施方式中的密钥生成过程,其实际上也示出了客户端登录服务端时二者的交互;

[0021] 图 3 至图 6 示出了本申请一种实施方式中的安全接口数据控制流程,其实际上也示出了客户端与服务端进行业务数据传输时二者的交互;

[0022] 图 7 示出了本申请一种实施方式用于车辆卡管理系统中的部分接口列表;

[0023] 图 8 示出了本申请一种实施方式中客户端和服务端之间的拓扑示意图。

具体实施方式

[0024] 本申请仍以车辆卡管理系统为例,对本申请提出的不使用 HTTPS 的数据安全传输方法及系统以及其涉及的客户端和服务端进行描述。可以理解的是,该方法和系统及其涉及的客户端和服务端也可以应用于广域物联网的其它应用中。

[0025] 对于车辆卡管理系统,需要考虑稳定性、安全性和易用性。因此,本申请在设计该车辆卡管理系统的方案中,对传输数据进行了多方面的考虑,例如引入了服务端自身认证的证书,来实现数据双向认证机制;又例如传输的用户数据使用对称加密技术,这样相比采用 HTTPS 协议的传输可以尽可能地提高效率;再例如还可以使用用户识别码,接口数据不包含用户信息内容,从而可以对用户信息给予保密;又例如还可以使接口参数和返回数据为字符串,从而传输数据与数据类型无关;再例如还可定制化接口数据传输的安全控制,即

定制是否需要加密传输数据。

[0026] 因此,在本申请的一种实施方式中,提出了不使用 HTTPS 的数据安全传输方法,该方法包括注册步骤、登录步骤和解密步骤。在注册步骤中,服务端在本地创建证书授权中心,并向相连的客户端颁发用户证书,用户证书用作客户端登录所述服务端的登录凭证;在登录步骤中,服务端在收到客户端的登录信息后,根据登录凭证分配密钥,并将密钥返回给客户端;在解密步骤中,服务端根据密钥加密或解密客户端发来的数据信息。

[0027] 具体地,对于注册步骤,首先服务端自己创建证书授权中心(CA),并在接收到所述客户端的注册信息时,向客户端颁发 CA 认证的用户证书,并保存客户端相关的信息及其对应的用户证书,一般地,客户端相关的信息至少包括该客户端的用户名和密码。

[0028] 对于登录步骤,当服务端接收客户端发送来的登录信息,通常登录信息包括客户端的用户名和密码,在本实施方式中,该密码为使用客户端的用户证书加密后的密文;然后,服务端根据用户名取得对应的用户证书,使用用户证书解密密文得到密码,然后随机产生密钥,保存密钥,并将密钥返回给客户端。当然,本步骤或者后续一些步骤中还可以涉及一些已知的技术手段,例如,在解密得到密码后,服务端将该密码和用户名与服务端事先存储的客户端相关的信息进行校验,如果校验通过,则继续后续步骤如产生密钥等,如果校验不通过,则可以向客户端发送用户名和密码不匹配之类的提示信息。

[0029] 在另一种实施方式中,除了具有上述实施方式的功能步骤外,登录步骤还可以包括生成识别步骤,对应地,解密步骤还可以包括用户识别步骤。在生成识别子步骤中,服务端根据登录凭证,生成用户识别码(也可以称之为用户登录校验码),并将用户识别码返回给客户端;在用户识别步骤中,服务端在接收到客户端发送的数据信息后,根据用户识别码确定数据信息对应的客户端,并响应对应的客户端。

[0030] 具体地,在生成识别步骤中,服务端在接收到客户端发送来的登录信息后,根据客户端的登录凭证随机产生用户识别码,保存用户识别码,并将用户识别码返回给客户端;而在用户识别步骤中,服务端在确定出数据信息对应的客户端后,获得对应的客户端的密钥。

[0031] 在又一种实施方式中,除了具有上述各实施方式的功能步骤外,本申请的不使用 HTTPS 协议的数据安全传输方法还可以包括接口定制步骤:服务端根据客户端的类型和业务功能提供安全接口信息,并向客户端公布安全接口信息,安全接口信息用于指示需要加解密操作的接口;当服务端接收到客户端发送来的携带有与安全接口信息相关内容的信息,结合该安全接口信息确定关于待传输数据的加解密操作。一种实施例中,安全接口信息包括安全接口列表,该安全接口列表中登记有需要对传输数据进行加解密操作的接口;另一种实施例中,安全接口信息包括带有安全参数值的接口函数,该安全参数值用于表征接口安全的级别。

[0032] 本申请还提供一种实施方式,其除了具有上述各实施方式的功能步骤外,对于传输于服务端和客户端之间的数据,其采用的数据格式为 JSON 数据交换格式。另一种实施方式中,服务端和客户端之间的加密数据使用 BASE64 进行编码后再传输。

[0033] 下面结合附图对本申请上述各实施方式作进一步详细说明。

[0034] 如图 2 所述,为在本申请一种实施方式提供的不使用 HTTPS 协议的数据安全传输方法中的密钥生成过程示意图,其实际上也示出了客户端登录服务端时二者的交互。

[0035] 客户端的用户使用用户名、密码进行用户登录。

[0036] 一种实施例中,登录接口如下定义。

[0037] // 摘要: 车辆卡系统登录接口,该接口不同于其它业务数据接口,接口参数只有一个。

[0038] // 用户登录,明文传输

[0039] //

[0040] // 参数:

[0041] //JSONData:JSON 数据序列化串,其中的用户密码节点使用了证书私钥加密后的 BASE64 编码串。

[0042] //

[0043] // 返回:

[0044] //JSON 数据串,其中返回的密钥 key 使用了证书公钥加密后的 BASE64 编码串

[0045] //

[0046] public string UserLogin(string JSONData);

[0047] 客户端用户登录成功后,返回的 JSON 数据串里包含了密钥 key 和用户识别码 (checkcode)。其中的登录过程涉及以下步骤 a) ~ d)。

[0048] 在步骤 a) 中,终端用户登录,将登录名、密码 (具体实现时,可以取的用户密码 MD5 哈希值,使用用户证书对哈希值进行加密,并对加密后的密文进行 BASE64 编码,故最终传输的密码为 BASE64 格式的伪码串) 以及其它登录信息,封装成 JSON 串,调用登录接口登录。

[0049] 在步骤 b) 中,服务端收到用户登录数据,解析 JSON 参数,根据用户名信息获取用户对应的证书,解密用户密码并验证。密码验证过程先进行 BASE64 解码得到密文,然后使用该用户对应的证书公钥解密密文,得到用户密码的 MD5 哈希值,与服务端上该用户保存的 MD5 哈希值比较,如果相同,则密码验证成功,如果不相同,则密码校验失败。

[0050] 在步骤 c) 中,服务端验证用户登录信息正确,随机产生一个密钥 key (字符串,由特殊符号、数字、字符组成) 并保存,并使用用户对应的证书 (证书公钥) 对 key 进行加密,将加密后的密文组装到返回的 JSON 数据中,同时在返回的 JSON 数据中还包含一个用户识别码 (checkcode,也是由服务端随机生成的,一种具体实现中,为了唯一性,使用的是 GUID);在接口返回的 JSON 数据结构中,都有一个 rt 的证书节点,该节点用于描述接口业务操作状况,如果操作成功 rt 为 0;失败则返回其它失败代号。

[0051] 在步骤 d) 中,客户端登录成功后收到返回数据,利用用户证书 (证书私钥) 解密密钥 key,这样就和服务端拥有相同的密钥 key,同时客户端需要保存用户识别码 checkcode。

[0052] 客户端登录成功后获得了密钥和用户识别,就可以使用服务端提供的接口进行业务操作,车辆卡系统业务操作接口如下设计样式。

[0053] // 以下两组代码片段用于展示车辆卡系统加密接口和未加密接口定义样式。

[0054] // 摘要: 车辆卡系统业务操作安全接口 (业务数据需要进行加密传输)

[0055] // 用户登出,参数和返回值需要进行加密传输

[0056] //

[0057] // 参数:

[0058] //JSONData: 原始内容为 JSON 序列化后的数据串,这里是加密后的 BASE64 编码串。JSON 数据节点信息,参见接口文档。

[0059] //checkcode: 用户登录产生的用户识别码。

[0060] //

[0061] // 返回 :

[0062] // 原始内容 JSON 数据串,这里是加密后的 BASE64 编码串。JSON 数据节点信息,参见接口文档。

[0063] //

[0064] public string UserLogout(string checkcode,string JSONData) ;

[0065] // 摘要 : 车辆卡系统业务操作接口

[0066] // 查询车辆基础信息,如车辆颜色、厂牌型号、类型等信息。

[0067] //

[0068] // 参数 :

[0069] //JSONData: 内容为 JSON 序列化后的数据串。JSON 数据节点信息,参见接口文档。

[0070] //checkcode: 用户登录产生的用户识别码。

[0071] //

[0072] // 返回 :

[0073] // 内容 JSON 数据串。JSON 数据节点信息,参见接口文档。

[0074] //

[0075] public string QueryVehicleInfo(string checkcode,string JSONData) ;

[0076] 对于安全接口,业务数据都是通过密文进行传输的,客户端和服务端使用相同密钥对业务数据进行加解密控制。

[0077] 如图 3 至图 6 所示,示出了本申请一种实施方式提供的不使用 HTTPS 协议的数据安全传输方法中的安全接口数据控制流程示意图,其实际上也示出了客户端与服务端进行业务数据传输时二者的交互,所涉及的交互大体涉及如下过程 a) ~ e)。

[0078] 在过程 a) 中,客户端用户将业务传输数据进行 JSON 序列化为字符串格式。

[0079] 在过程 b) 中,客户端调用服务端接口,根据服务端接口定义,判断接口的数据传输是否需要进行加密,对需要加密传输的业务数据使用密钥 key 进行对称加密。客户端业务数据请求接口,由两个字符串型参数组成,第一个参数是客户端登录的用户识别码,第二个是实际的业务数据,如果是安全接口,需要对该业务数据进行加密。由于加密后的密文是不规则数据,为了接口类型统一,需要对密文进行 BASE64 编码,即实际传输的业务数据参数是经过 BASE64 编码后的字符串内容。

[0080] 在过程 c) 中,服务端收到客户端的业务数据请求,根据响应的接口位置,可直接判断是否是安全控制接口,如果是安全控制接口,利用用户识别码得到客户端用户的密钥 key,然后对业务数据进行 BASE64 解码、使用密钥 key 解密密文,最终得到实际的 JSON 数据字符串,接着进行 JSON 反序列化及进行一系列的业务操作。

[0081] 在过程 d) 中,服务端业务操作完成后,JSON 序列化接口返回数据,如果是安全接口,使用密钥 key 对 JSON 序列化后的字符串进行对称加密,并对加密后的密文进行 BASE64 编码;如果不是安全接口,则直接返回 JSON 串。

[0082] 在过程 e) 中, 终端用户收到返回的数据, 如果调用的是安全接口, 首先需要 BASE64 解码, 然后使用密钥 key 进行解密得到服务端返回的 JSON 数据串; 如果不是调用安全接口, 返回的数据就是实际的业务数据 JSON 串。

[0083] 具体地, 在客户端已经登录服务端后, 图 3 是不需要考虑数据安全时客户端与服务端的交互过程: 首先客户端将 JSON 格式的接口数据不加密地传输给服务端, 服务端在接收到该明文的接口数据后, 根据接口类型进行业务数据处理, 并进行车辆卡核心业务逻辑处理, 然后对业务处理后产生的数据进行 JSON 格式打包, 并不使用安全控制 (即不需要进行加密处理) 直接返回明文数据给客户端。

[0084] 图 4 与图 3 的不同之处在于, 图 4 的服务端在对业务处理后产生的数据进行 JSON 格式打包 (简称 JSON 串数据) 后需要进行安全控制 (即需要进行加密处理以防止非请求的客户端或其它第三方获知业务数据信息), 此时, 服务端使用与该请求数据的客户端对应的密钥加密 JSON 串数据, 形成密文, 并对密文进行 BASE64 编码, 得到伪串并将伪串通过反馈给客户端; 客户端对接收到的伪串进行 BASE64 解码得到密文, 然后用之前存储的密钥 (即客户端登录服务器后服务器反馈给客户端的密钥) 解密密文, 从而得到明文形式的业务数据信息。

[0085] 图 5 与图 3 的不同之处在于, 客户端在发送数据信息 (例如车辆卡相关的业务数据) 时需要加密处理后再传输, 即客户端首先使用密钥 (即客户端登录服务器后服务器反馈给客户端的密钥) 加密数据, 得到密文, 然后对密文进行 BASE64 进行编码, 形成伪串, 然后调用接口函数将伪串发送给服务端, 该接口函数中的参数涉及客户端的用户识别码 (即 checkcode) 和编码后的伪串。

[0086] 图 6 中, 客户端和服务端在数据传输的安全性上要求很高, 即客户端需要加密传输, 而服务端在处理业务后也需要进行安全控制, 以安全地将数据传输回客户端。客户端和服务端具体加密的过程类似前述相关描述, 在此不再详述。

[0087] 通过以上描述可知, 本申请提出了使用一种 Webserver 服务器, 基于 HTTP 协议对传输数据进行定制化加密的数据安全传输的方案, 该方案提高了传输效率和简化了加解密流程, 加密数据传输接口可随意定制和扩展。

[0088] 首先, 本申请的一个特点是引入证书。每个客户端用户都应该有一个自己的用户证书, 该证书由服务端颁发。证书的 CA 由服务端自己创建的, 在整个车辆卡系统中唯一, 所有的用户证书由该 CA 颁发。用户证书不仅是车辆卡终端用户的凭证, 而且是数据加密传输的双向认证。客户端使用用户证书的私钥加密 (解密) 数据, 服务端使用客户端对应的公钥进行解密 (加密) 数据, 即实现了传输数据的双向认证。

[0089] 其次, 本申请采用了对称加密。对称加解密技术, 需要服务端和客户端使用一个相同的密钥 (key)。用户登录时, 服务端随机分配一个密钥, 利用证书双向认证机制, 返回给客户端, 这样双方都有一个相同的密钥。当然用户每次登录后的密钥都是不一样的。对称加密比使用证书双向认证加密效率要高得多, 在车辆卡系统中, 对基本的业务数据安全接口, 都是使用对称加密的方法。

[0090] 接着, 本申请引入用户识别码。服务端对于客户端请求的 Webserver 接口, 并不知道每次过来的数据是由哪个客户端请求的, 简单的做法是每次数据请求都包含客户端的用户信息, 这样用户的信息就很容易被暴露了。识别码是客户端用户登录成功后, 服务端分配

给用户的一个唯一编码。客户端用户使用识别码请求业务数据,这样服务端可以通过识别码知道该条数据的来源,就可以针对具体的用户进行业务操作。

[0091] 然后,本申请在接口参数和返回定义字符串类型做出了改进。Webserver 的接口和普通的函数接口使用方式基本一致,通常使用接口时,会根据不同的数据类型使用多个接口参数。而本申请的车辆卡管理系统的接口,对传输的业务数据使用一个接口参数,类型统一为字符串类型,但是该字符串类型比较特殊,它是由 JSON 序列化后组装成的,同样返回的数据也是 JSON 序列化后的字符串。这样做的好处,接口不关心具体的数据类型,对于业务数据的修改不会影响接口定义;方便数据的加解密,整体性好。

[0092] 不管是加密的数据和未加密的数据,最终都是 JSON 数据展现的。每个接口的 JSON 数据是不一样的,有一个标准接口文档作为参考,在文档里面,制定了每个接口的 JSON 数据拼装规则,不同的节点表示不同的数据类型。当服务端收到客户端的 JSON 数据包时,会根据当前接口对应的标准解析 JSON 数据,提取需要的数据进行业务处理。

[0093] 最后,本申请还可以定制安全接口。在车辆卡管理系统中,服务端根据客户端类型和业务功能拥有大量的接口,每一个接口处理不同的业务。而在使用接口进行数据传输过程中,需要对某些传输数据进行加密传输,对于服务端和客户端如何知道哪些接口的数据需要进行加密,本申请提供了两种解决方案。

[0094] 其中之一是采用列表方式。虽然车辆卡系统中的接口繁多,但是可以确定需要加密传输的接口,将需要加密传输的接口认为是安全接口,登记为一个列表,服务端发布时公布其安全接口列表,这样客户端使用安全接口时,就需要对传输数据进行加解密操作。

[0095] 另一种方案是为接口函数增加一个参数,专门标注接口安全级别,如 0 表示未进行业务数据加密;1 表示使用了 key 对称加密;2 表示使用了非对称加密。这样服务端就可以根据该参数值确定业务数据是否需要解密,和解密方式。

[0096] 为便于理解,如图 7 所示,这里以列表方式列出了车辆卡管理系统中部分接口说明。

[0097] 基于以上方法实施方式,本申请一种实施方式还提出了一种使用如上方法实现的不使用 HTTPS 协议的数据安全传输系统,图 8 示出了该系统中客户端和服务端的拓扑结构示意图。另一种实施方式还提出了用于上述方法的客户端和/或服务端。

[0098] 综上,本申请实施方式提出的不使用 HTTPS 协议的数据安全传输方法具有如下优点:

[0099] 1) 使用 HTTP 传输协议,实现了类似 HTTPS 的功能;

[0100] 2) 使用 JSON 序列化业务数据传输,单一的传输参数,与接口类型无关性,数据内容灵活控制,易于后期接口的维护升级;

[0101] 3) 可定制安全接口,对需要进行安全控制的接口进行加密,不需要安全控制的接口可以直接进行明文传输;

[0102] 4) 方案容易实施,使用简单。

[0103] 本领域技术人员可以理解,上述实施方式中各种方法的全部或部分步骤可以通过程序来指令相关硬件完成,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:只读存储器、随机存储器、磁盘或光盘等。

[0104] 以上内容是结合具体的实施方式对本发明所作的进一步详细说明,不能认定本发

明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干简单推演或替换。

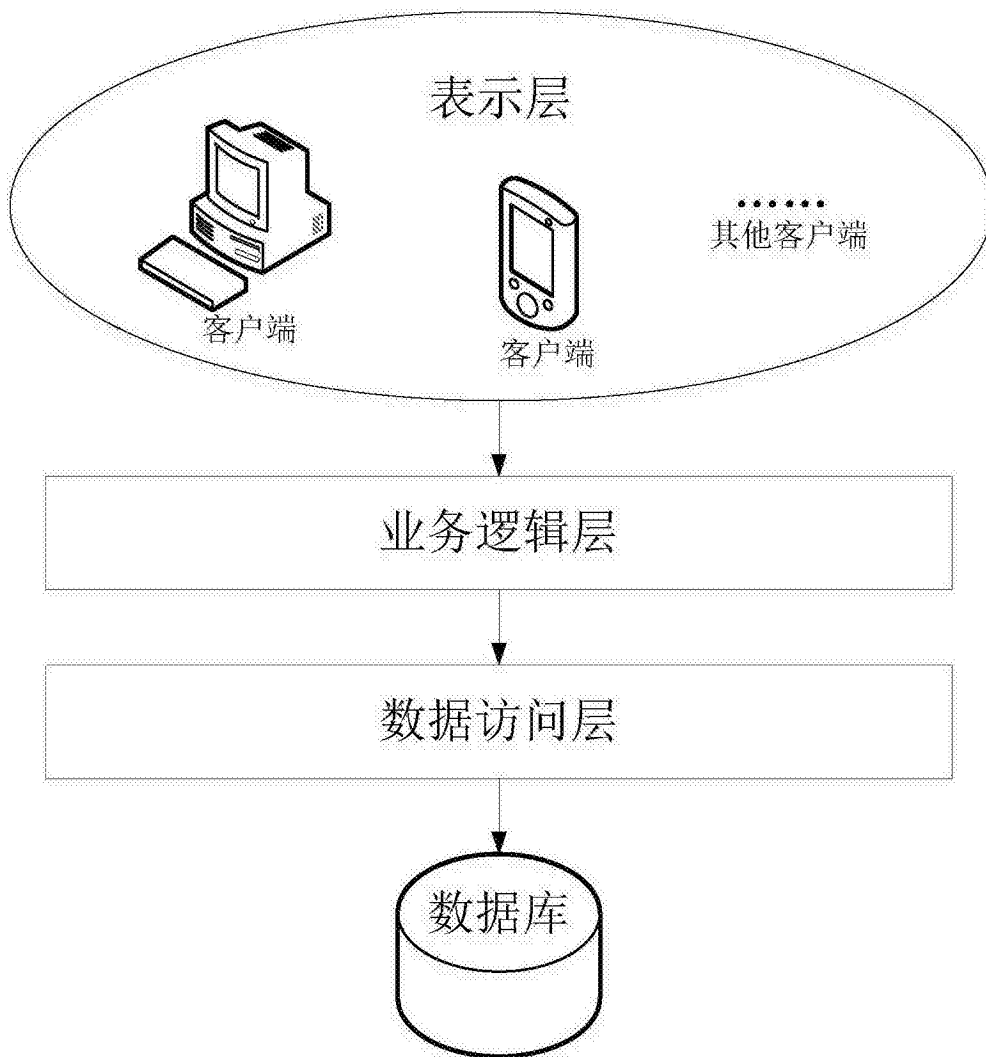


图 1

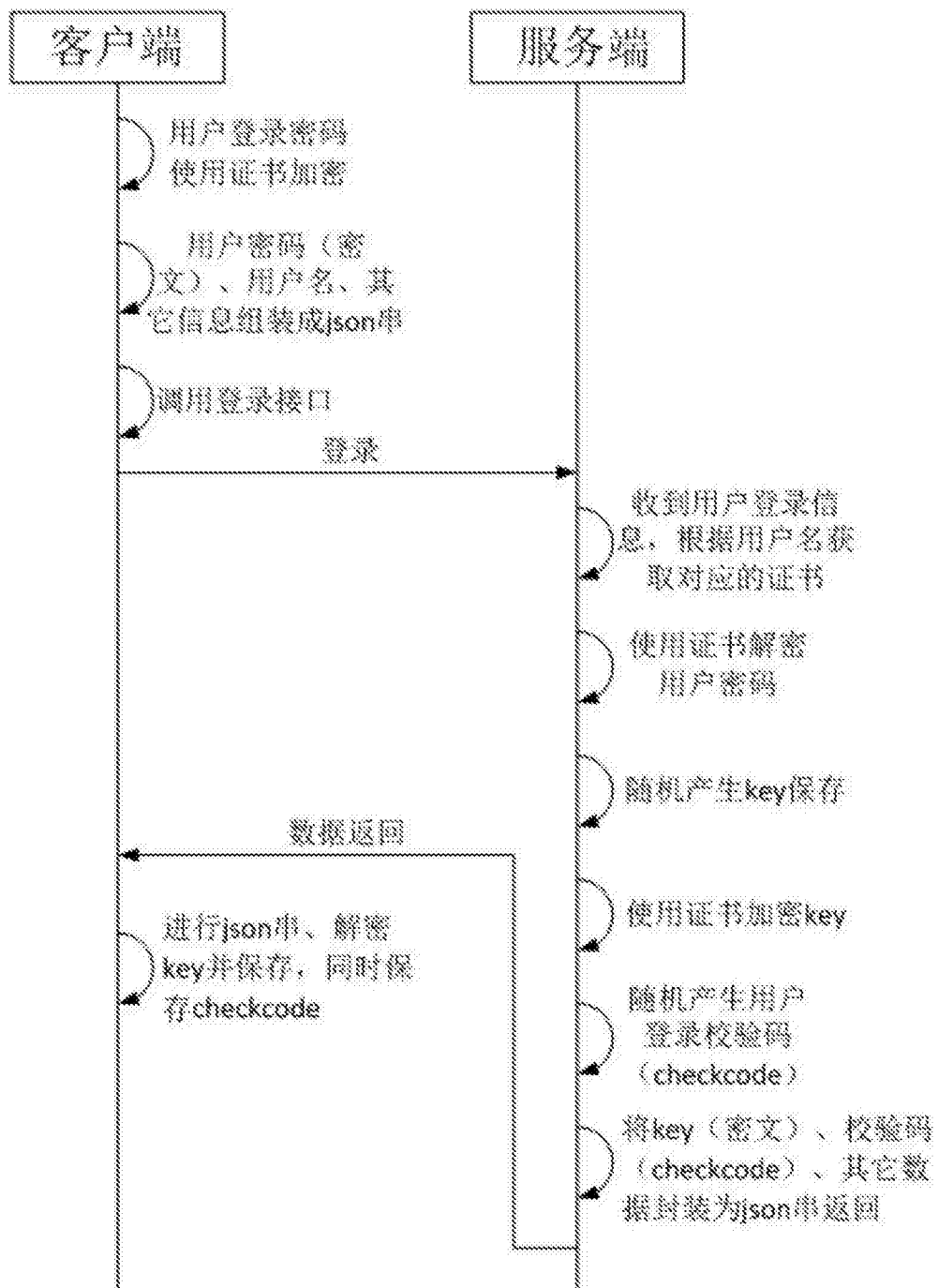


图 2

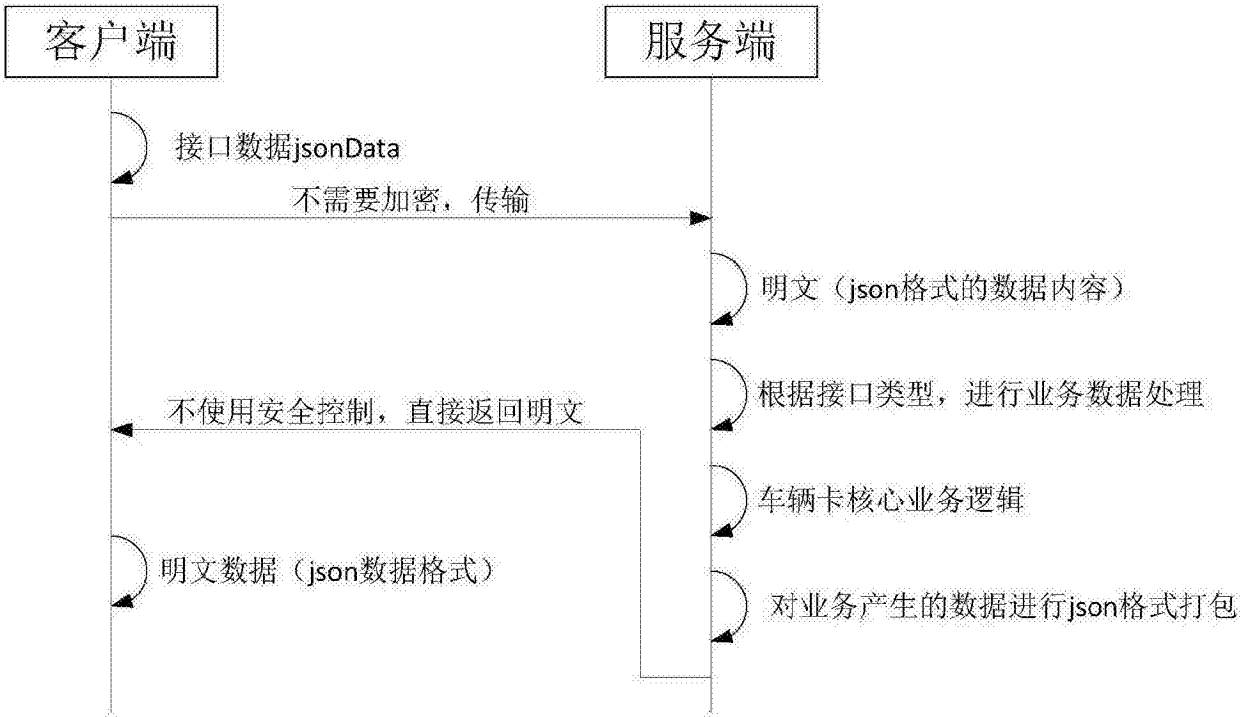


图 3

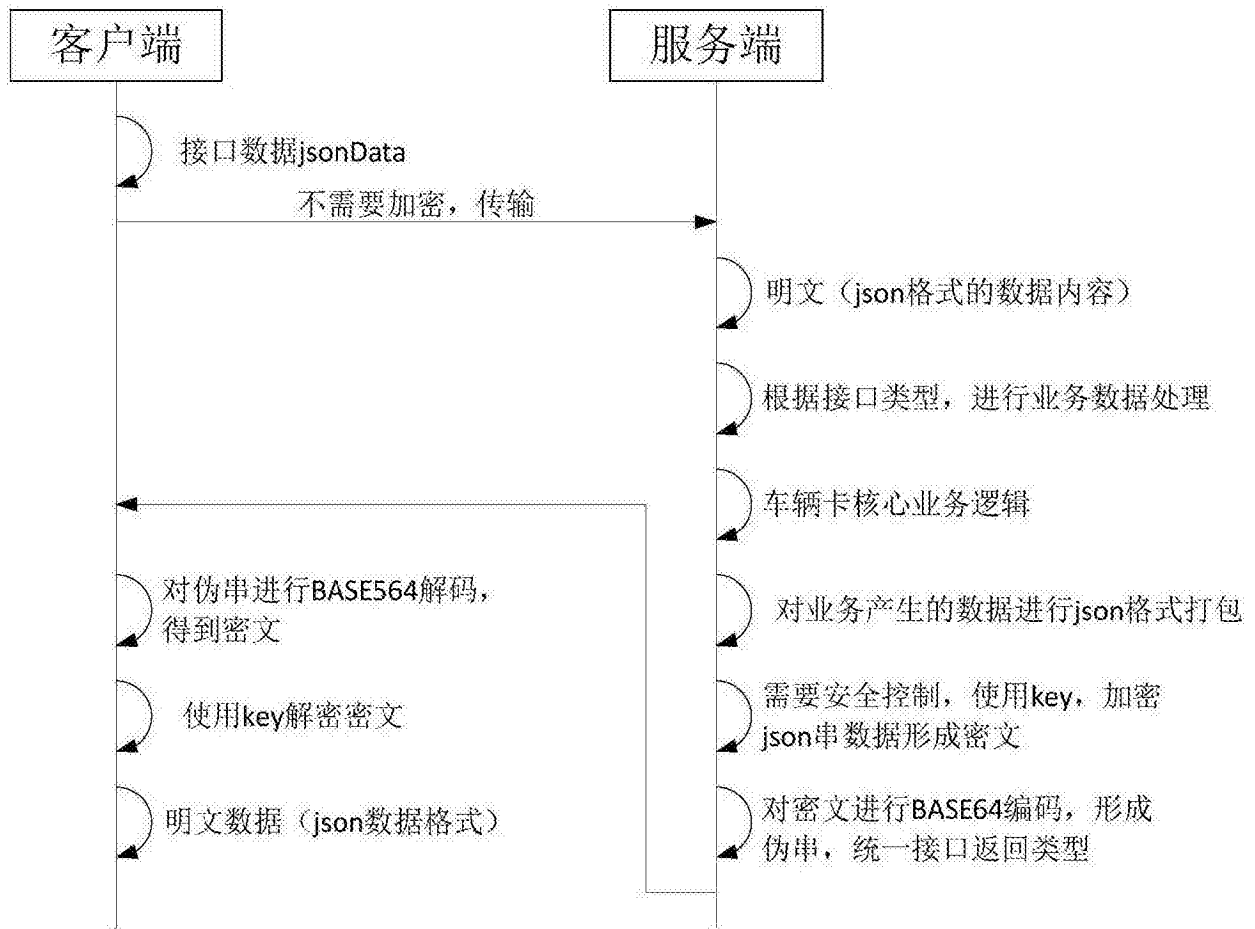


图 4

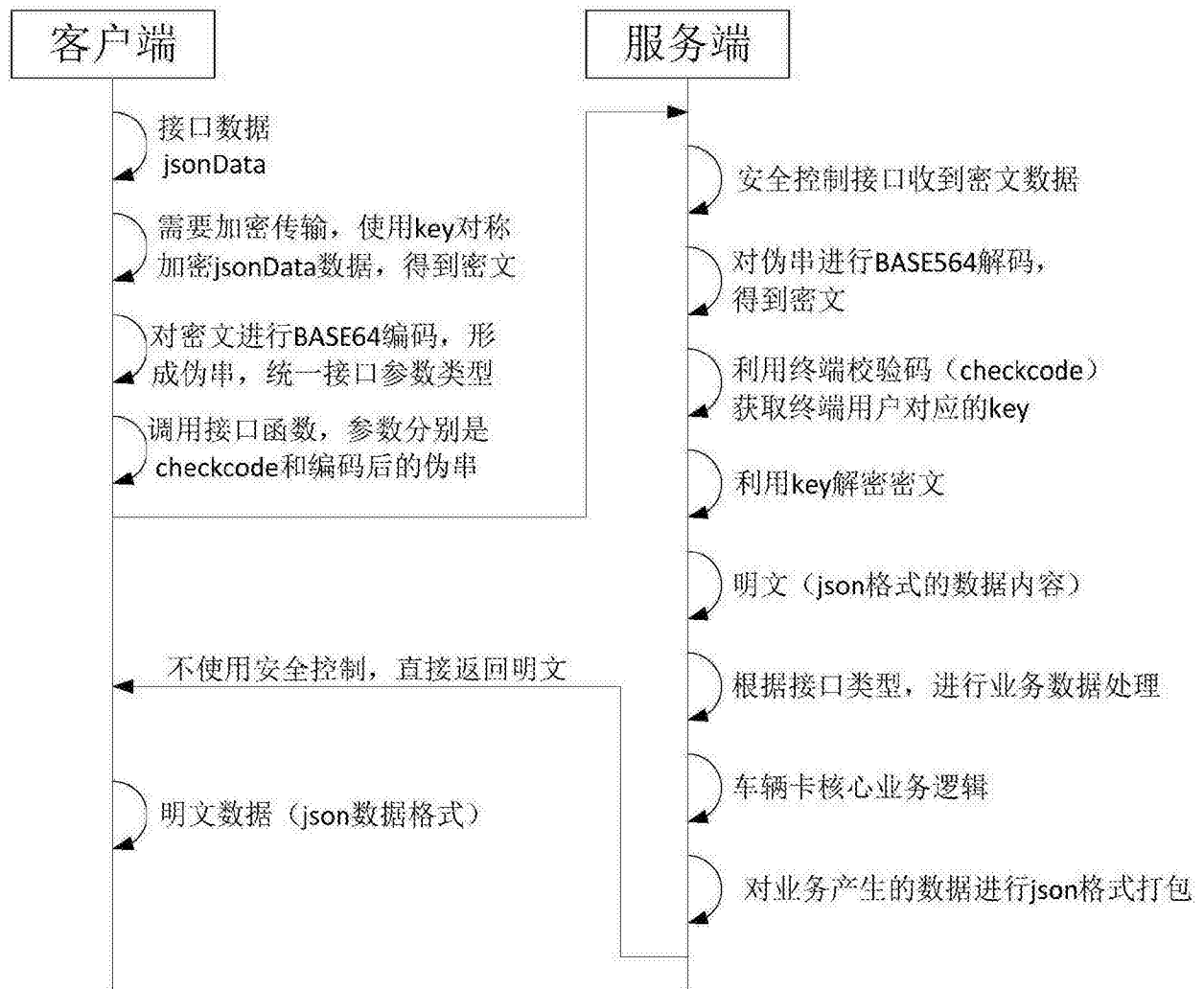


图 5

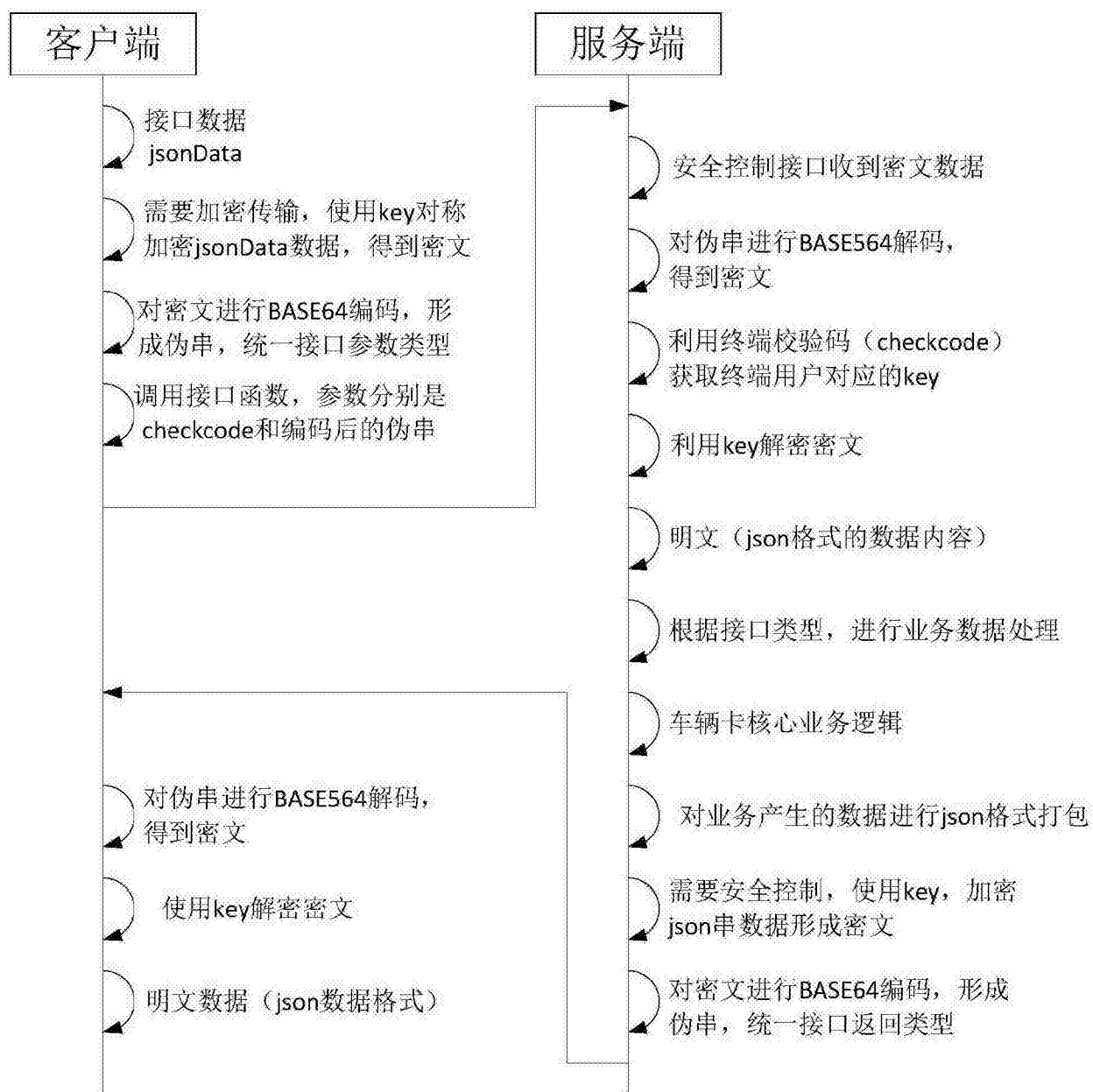


图 6

接口名称	是否加密	说明
UserPrivilegeList	是	获取用户权限列表
UserLowerOrgcodeList	是	获取下级单位列表
AddUser	是	添加新用户
DeleteUser	是	用户注销
QueryUser	是	查询用户
LogoutUser	是	用户登出
HeartBeatPing	是	终端设备心跳包
AddOil	否	添加油料基础数据
AddRepair	否	添加修理类型基础数据
IssueCard	是	车辆卡发行登记
PlanMaterialReported	是	上报器材计划
...		

图 7

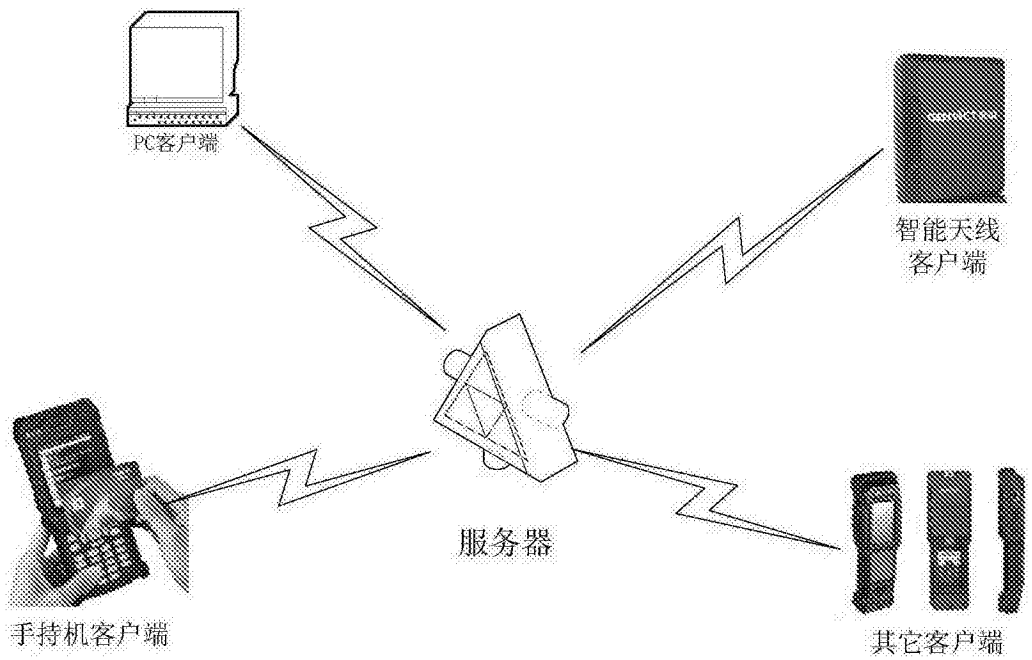


图 8