



(12)发明专利申请

(10)申请公布号 CN 109041055 A

(43)申请公布日 2018.12.18

(21)申请号 201810847626.4

(22)申请日 2018.07.27

(71)申请人 马占朝

地址 054000 河北省邢台市桥西区钢铁北路41号省公路工程局

(72)发明人 马占朝

(51)Int. Cl.

H04W 12/02(2009.01)

H04W 88/16(2009.01)

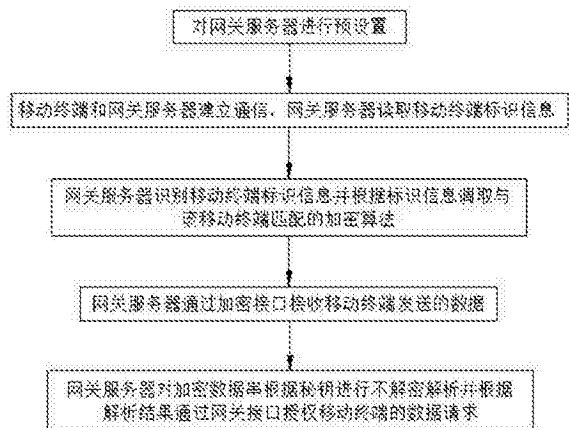
权利要求书2页 说明书4页 附图4页

(54)发明名称

一种用于金融安防环境的移动终端与网关服务器传输方法

(57)摘要

本发明公开了一种用于金融安防环境的移动终端与网关服务器传输方法,该方法包括以下步骤:S1、对网关服务器进行预设置;S2、移动终端和网关服务器建立通信,网关服务器读取移动终端标识信息;S3、网关服务器识别移动终端标识信息并根据标识信息调取与该移动终端匹配的加密算法;S4、网关服务器通过加密接口接收移动终端发送的数据;S5、网关服务器对加密数据串根据秘钥进行不解密解析并根据解析结果通过网关接口授权移动终端的数据请求。本发明用于金融安防环境的移动终端与网关服务器传输方法对移动终端和网关服务器传输过程进行数据加密,具有很好的数据安全性。



1. 一种用于金融安防环境的移动终端与网关服务器传输方法,其特征在于,该方法包括以下步骤:

S1、对网关服务器进行预设置;

S2、移动终端和网关服务器建立通信,网关服务器读取移动终端标识信息;

S3、网关服务器识别移动终端标识信息并根据标识信息调取与该移动终端匹配的加密算法;

S4、网关服务器通过加密接口接收移动终端发送的数据;

S5、网关服务器对加密数据串根据密钥进行不解密解析并根据解析结果通过网关接口授权移动终端的数据请求。

2. 根据权利要求1所述的一种用于金融安防环境的移动终端与网关服务器传输方法,其特征在于,所述S1对网关服务器进行预设置包括:

S11、网关服务器预设网关接口、数据同步接口和加密接口;

S12、网关服务器根据网络数据建立移动终端标识信息库,该信息库中预设有不同的标识信息对应的不同的加密算法;

S13、网关服务器预设加密算法加密后密钥的密码数据库,该密码数据库存储各密钥对应的数据编码字符,该字符代表指定的数据信息。

3. 根据权利要求1所述的一种用于金融安防环境的移动终端与网关服务器传输方法,其特征在于,所述移动终端和网关服务器建立通信包括:

S21、移动终端生成通信请求,通过网关接口和数据同步接口向网关服务器发送通信请求;

S22、网关服务器对移动终端的通信请求进行验证;

S23、数据同步接口控制网关服务器与移动终端进行数据通信,网关接口控制移动终端建立通信后的数据下载和上传。

4. 根据权利要求3所述的一种用于金融安防环境的移动终端与网关服务器传输方法,其特征在于,所述网关服务器对移动终端的通信请求进行验证包括:

S221、网关服务器读取通信请求并根据通信标准进行请求验证;

S222、当验证通过时,网关接口下发进一步操作指令至移动终端;

S223、当验证未通过时,网关接口下发验证失败指令至移动终端以重新进行通信请求发送。

5. 根据权利要求1所述的一种用于金融安防环境的移动终端与网关服务器传输方法,其特征在于,所述网关服务器识别移动终端标识信息并根据标识信息调取与该移动终端匹配的加密算法包括:

S31、网关服务器通过数据同步接口识别获取移动终端的标识信息,该标识信息为具有该移动终端数据建立方式的设备类型信息;

S32、网关服务器根据所述S1预设置的终端标识信息库和获取的标识信息进行匹配调取适用于该移动终端的加密算法;

S33、将调取的加密算法嵌入网关服务器的加密接口。

6. 根据权利要求1所述的一种用于金融安防环境的移动终端与网关服务器传输方法,其特征在于,所述网关服务器通过加密接口接收移动终端发送的数据包括:

S41、移动终端生成数据,并将数据分割为帧长度相等的帧;

S42、移动终端向网关服务器发送数据帧,该数据帧通过加密接口进行加密;

S43、网关服务器获取加密后的数据帧。

7. 根据权利要求1所述的一种用于金融安防环境的移动终端与网关服务器传输方法,其特征在于,所述网关服务器对加密数据串根据密钥进行不解密解析并根据解析结果通过网关接口授权移动终端的数据请求包括:

S51、网关服务器对接收的加密数据帧与所述的S1建立的密码数据库进行比对;

S52、对获取加密后的数据帧密钥进行指令匹配完成不解密密码解析;

S52、通过网关服务器预设的密钥对应的指令信息授权移动终端的数据请求。

一种用于金融安防环境的移动终端与网关服务器传输方法

技术领域

[0001] 本发明涉及数据通信安全技术领域,具体是用于金融安防环境的移动终端与网关服务器传输方法。

背景技术

[0002] 数据通信的安全随着互联网技术的发展越来越重要,特别是现如今互联网金融蓬勃发展的时代。在互联网金融所涉及的范围内,移动终端往往占据了重要的地位,其涉及到金融安防监控、电子账户交易等。所以,移动终端与网关服务器传输的安全变得尤为重要。

[0003] 现有技术CN107800699A提供了一种用于金融安防环境的移动终端与网关服务器传输方法,包括以下步骤:移动终端和网关服务器的预设置,对移动终端和网关服务器均进行离线数据传输预设;移动终端与网关服务器通信状态的建立,通过移动终端发送通信请求,建立其与网关服务器的通信连接;移动终端将数据发送给网关服务器,移动终端对数据进行消息体分割后,发送给网关服务器;网关服务器接收移动终端发送的消息体,并对消息体进行组合。该技术通过移动终端和网关服务器建立通信后发送分割后的数据信息至网关服务器实现了数据通信。但是,在互联网技术日益发达的时代,简单的数据分割处理并不能保证数据信息的安全性,分割后的消息体更易被破解导致金融环境丧失安全性。

发明内容

[0004] 本发明的目的在于提供一种用于金融安防环境的移动终端与网关服务器传输方法,以解决上述背景技术中提出的现有的用于金融安防环境的移动终端与网关服务器传输方法数据传输数据安全性差、数据处理简单、金融安防环境安全性差的问题。

[0005] 为实现上述目的,本发明提供如下技术方案:

[0006] 一种用于金融安防环境的移动终端与网关服务器传输方法,该方法包括以下步骤:

[0007] S1、对网关服务器进行预设置;

[0008] S2、移动终端和网关服务器建立通信,网关服务器读取移动终端标识信息;

[0009] S3、网关服务器识别移动终端标识信息并根据标识信息调取与该移动终端匹配的加密算法;

[0010] S4、网关服务器通过加密接口接收移动终端发送的数据;

[0011] S5、网关服务器对加密数据串根据密钥进行不解密解析并根据解析结果通过网关接口授权移动终端的数据请求。

[0012] 优选的,所述S1对网关服务器进行预设置包括:

[0013] S11、网关服务器预设网关接口、数据同步接口和加密接口;

[0014] S12、网关服务器根据网络数据建立移动终端标识信息库,该信息库中预设有不同的标识信息对应的不同的加密算法;

[0015] S13、网关服务器预设加密算法加密后密钥的密码数据库,该密码数据库存储各秘

钥对应的数据编码字符,该字符代表指定的数据信息。

[0016] 优选的,所述移动终端和网关服务器建立通信包括:

[0017] S21、移动终端生成通信请求,通过网关接口和数据同步接口向网关服务器发送通信请求;

[0018] S22、网关服务器对移动终端的通信请求进行验证;

[0019] S23、数据同步接口控制网关服务器与移动终端进行数据通信,网关接口控制移动终端建立通信后的数据下载和上传。

[0020] 更为优选的,所述网关服务器对移动终端的通信请求进行验证包括:

[0021] S221、网关服务器读取通信请求并根据通信标准进行请求验证;

[0022] S222、当验证通过时,网关接口下发进一步操作指令至移动终端;

[0023] S223、当验证未通过时,网关接口下发验证失败指令至移动终端以重新进行通信请求发送。

[0024] 优选的,所述网关服务器识别移动终端标识信息并根据标识信息调取与该移动终端匹配的加密算法包括:

[0025] S31、网关服务器通过数据同步接口识别获取移动终端的标识信息,该标识信息为具有该移动终端数据建立方式的设备类型信息;

[0026] S32、网关服务器根据所述S1预设置的终端标识信息库和获取的标识信息进行匹配调取适用于该移动终端的加密算法;

[0027] S33、将调取的加密算法嵌入网关服务器的加密接口。

[0028] 优选的,所述网关服务器通过加密接口接收移动终端发送的数据包括:

[0029] S41、移动终端生成数据,并将数据分割为帧长度相等的数据帧;

[0030] S42、移动终端向网关服务器发送数据帧,该数据帧通过加密接口进行加密;

[0031] S43、网关服务器获取加密后的数据帧。

[0032] 优选的,所述网关服务器对加密数据串根据密钥进行不解密解析并根据解析结果通过网关接口授权移动终端的数据请求包括:

[0033] S51、网关服务器对接收的加密数据帧与所述S1建立的密码数据库进行比对;

[0034] S52、对获取加密后的数据帧密钥进行指令匹配完成不解密密码解析;

[0035] S52、通过网关服务器预设的密钥对应的指令信息授权移动终端的数据请求。

[0036] 与现有技术相比,本发明的有益效果是:

[0037] 1) 本发明通过网关服务器接收移动终端连接请求和通过网关接口与数据同步接口与移动终端建立连接,实现了移动终端和网关服务器的数据传输;

[0038] 2) 本发明通过对移动终端进行标识识别并通过匹配该移动终端的加密算法对该移动终端发送的数据进行加密,结合网关服务器对加密后的密钥进行不解密解析完成数据识别与移动终端进行数据交互,提高了数据传输过程中数据的安全性和实现了金融安防环境的安全性的保证。

附图说明

[0039] 图1为本发明一种用于金融安防环境的移动终端与网关服务器传输方法的流程框图;

[0040] 图2为本发明一种用于金融安防环境的移动终端与网关服务器传输方法S1的具体步骤流程图；

[0041] 图3为本发明一种用于金融安防环境的移动终端与网关服务器传输方法S2的具体步骤流程图；

[0042] 图4为本发明一种用于金融安防环境的移动终端与网关服务器传输方法S22的具体步骤流程图；

[0043] 图5为本发明一种用于金融安防环境的移动终端与网关服务器传输方法S3的具体步骤流程图；

[0044] 图6为本发明一种用于金融安防环境的移动终端与网关服务器传输方法S4的具体步骤流程图；

[0045] 图7为本发明一种用于金融安防环境的移动终端与网关服务器传输方法S5的具体步骤流程图。

具体实施方式

[0046] 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。

[0047] 如图1所示,一种用于金融安防环境的移动终端与网关服务器传输方法,该方法包括以下步骤:

[0048] S1、对网关服务器进行预设置;如图2所示,其具体步骤如下:

[0049] S11、网关服务器预设网关接口、数据同步接口和加密接口;

[0050] S12、网关服务器根据网络数据建立移动终端标识信息库,该信息库中预设有不同的标识信息对应的不同的加密算法;

[0051] S13、网关服务器预设加密算法加密后密钥的密码数据库,该密码数据库存储各密钥对应的数据编码字符,该字符代表指定的数据信息。

[0052] S2、移动终端和网关服务器建立通信,网关服务器读取移动终端标识信息;如图3所示,其具体步骤如下:

[0053] S21、移动终端生成通信请求,通过网关接口和数据同步接口向网关服务器发送通信请求;

[0054] S22、网关服务器对移动终端的通信请求进行验证;如图4所示,具体步骤如下:

[0055] S221、网关服务器读取通信请求并根据通信标准进行请求验证;

[0056] S222、当验证通过时,网关接口下发进一步操作指令至移动终端;

[0057] S223、当验证未通过时,网关接口下发验证失败指令至移动终端以重新进行通信请求发送。

[0058] S23、数据同步接口控制网关服务器与移动终端进行数据通信,网关接口控制移动终端建立通信后的数据下载和上传。

[0059] S3、网关服务器识别移动终端标识信息并根据标识信息调取与该移动终端匹配的加密算法;如图5所示,其具体步骤如下:

[0060] S31、网关服务器通过数据同步接口识别获取移动终端的标识信息,该标识信息为具有该移动终端数据建立方式的设备类型信息;

[0061] S32、网关服务器根据所述S1预设的终端标识信息库和获取的标识信息进行匹配调取适用于该移动终端的加密算法;

[0062] S33、将调取的加密算法嵌入网关服务器的加密接口。

[0063] S4、网关服务器通过加密接口接收移动终端发送的数据;如图6所示,其具体步骤如下:

[0064] S41、移动终端生成数据,并将数据分割为帧长度相等的数据帧;

[0065] S42、移动终端向网关服务器发送数据帧,该数据帧通过加密接口进行加密;

[0066] S43、网关服务器获取加密后的数据帧。

[0067] S5、网关服务器对加密数据串根据密钥进行不解密解析并根据解析结果通过网关接口授权移动终端的数据请求;如图7所示,其具体步骤如下:

[0068] S51、网关服务器对接收的加密数据帧与所述S1建立的密码数据库进行比对;

[0069] S52、对获取加密后的数据帧密钥进行指令匹配完成不解密密钥解析;

[0070] S52、通过网关服务器预设的密钥对应的指令信息授权移动终端的数据请求。

[0071] 网关服务器通过对加密密钥在密码数据库中的匹配,匹配该加密数据对应的数据请求,复杂数据处理过程,对加密后的数据帧无需进行解密算法解密的步骤,实现数据处理过程的安全性,实现了金融安防环境的移动终端和网关服务器传输的安全提高。

[0072] 尽管已经示出和描述了本发明的实施例,对于本领域的普通技术人员而言,可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型,本发明的范围由所附权利要求及其等同物限定。

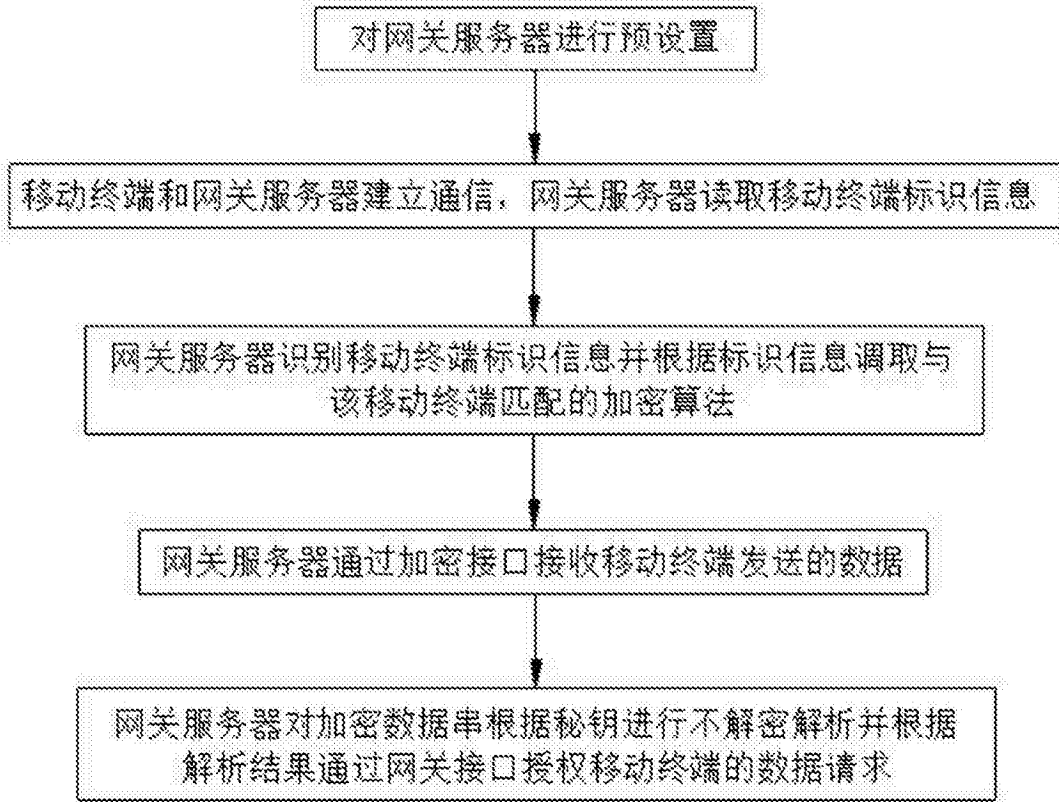


图1

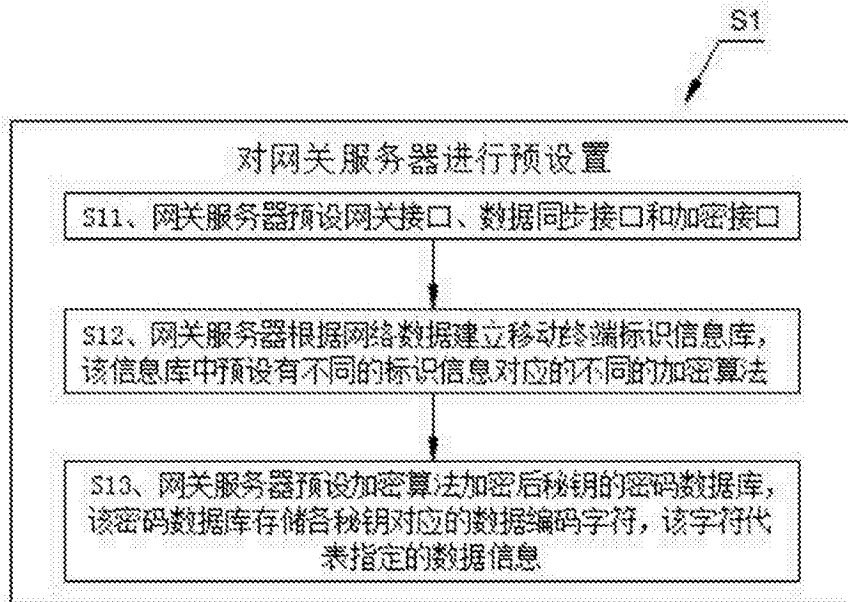


图2

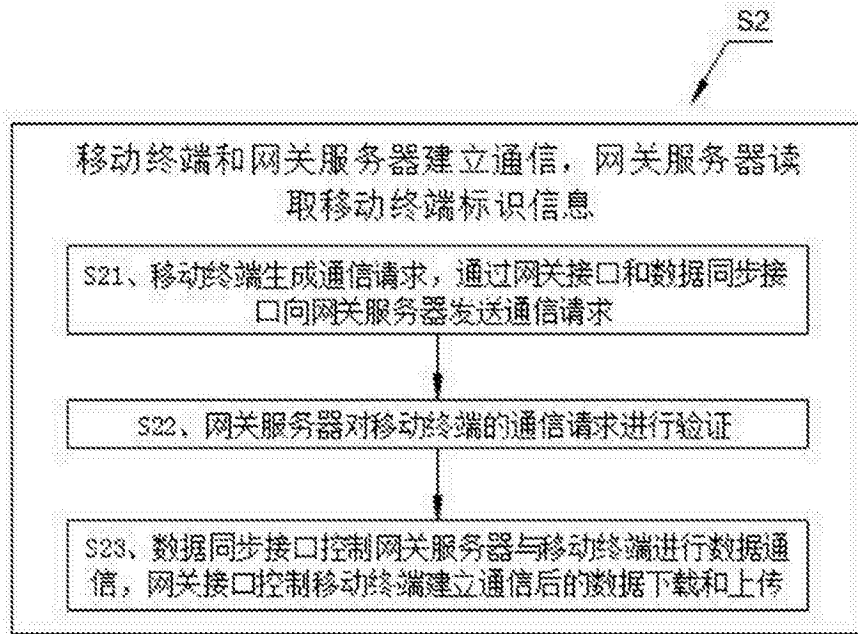


图3

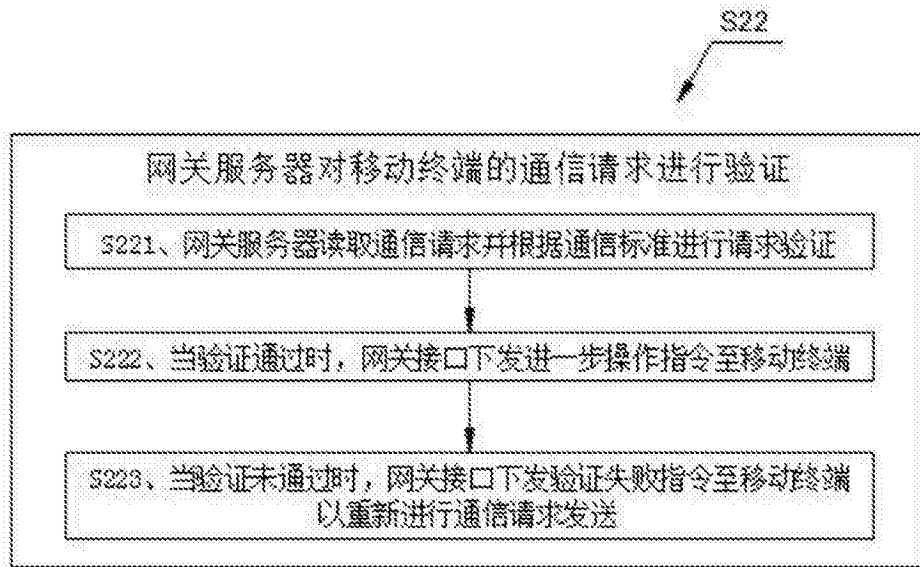


图4

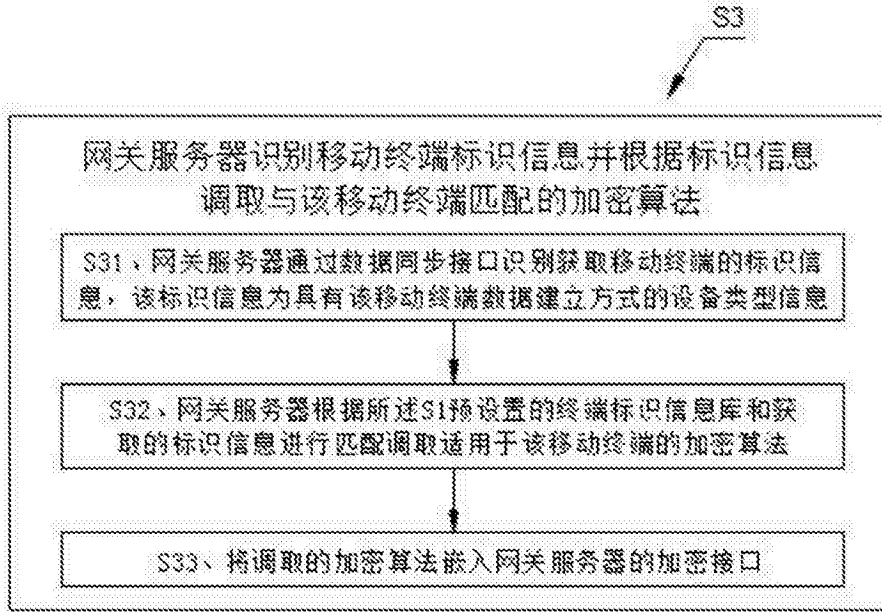


图5

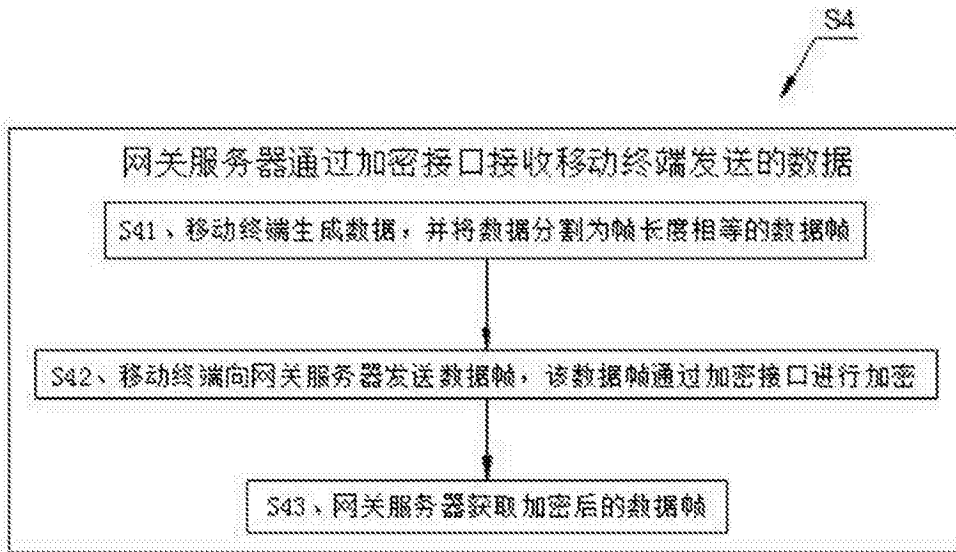


图6

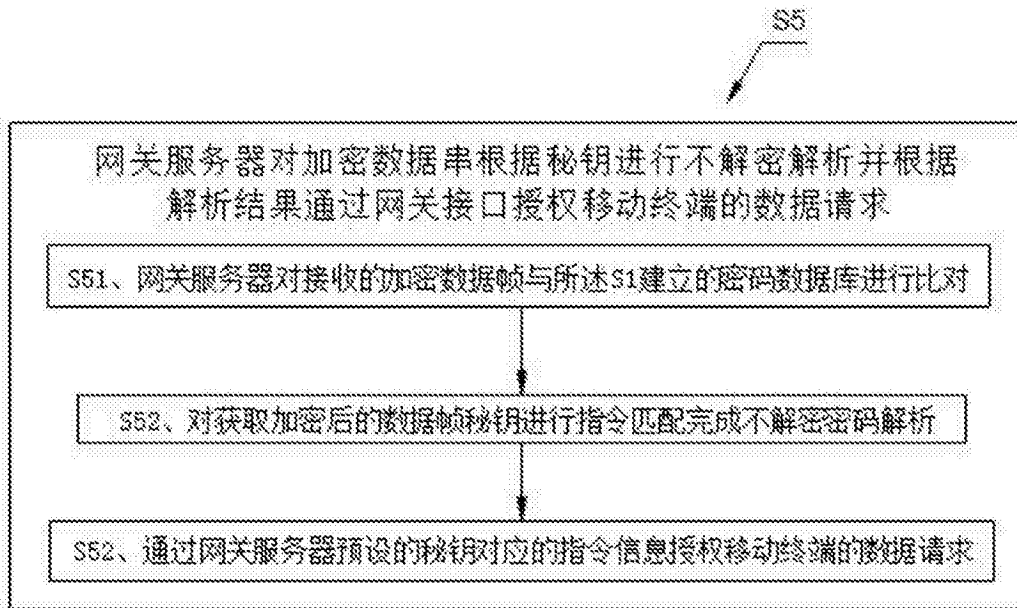


图7