



(12) 发明专利

(10) 授权公告号 CN 103024744 B

(45) 授权公告日 2015. 08. 05

(21) 申请号 201210568577. 3

CN 102111755 A, 2011. 06. 29,

(22) 申请日 2012. 12. 24

EP 2352321 A1, 2011. 08. 03,

CN 101166333 A, 2008. 04. 23,

(73) 专利权人 百度在线网络技术(北京)有限公司

审查员 靳莉

地址 100085 北京市海淀区上地十街 10 号
百度大厦三层

(72) 发明人 刘娟

(74) 专利代理机构 北京清亦华知识产权代理事
务所(普通合伙) 11201

代理人 宋合成

(51) Int. Cl.

H04W 12/06(2009. 01)

H04L 29/08(2006. 01)

(56) 对比文件

CN 102752269 A, 2012. 10. 24,

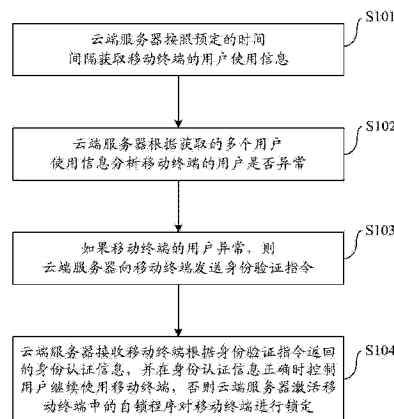
权利要求书2页 说明书5页 附图2页

(54) 发明名称

移动终端的身份验证的方法和系统

(57) 摘要

本发明提出一种移动终端的身份验证的方法和系统,其中所述方法包括以下步骤:云端服务器按照预定的时间间隔获取移动终端的用户使用信息;云端服务器根据获取的多个用户使用信息分析移动终端的用户是否异常;如果移动终端的用户异常,则云端服务器向移动终端发送身份验证指令;以及云端服务器接收移动终端根据身份验证指令返回的身份认证信息,并在身份认证信息正确时控制用户继续使用移动终端,否则云端服务器激活移动终端中的自锁程序对移动终端进行锁定。根据本发明实施例的方法,可以根据用户的使用习惯对移动终端的用户进行身份认证,有效防止移动终端丢失或者被盗时的用户隐私泄露,保证信息安全,提升用户体验。



1. 一种移动终端的身份验证的方法,其特征在于,包括以下步骤:

a、云端服务器按照预定的时间间隔获取移动终端的用户使用信息;

b、所述云端服务器根据获取的多个所述用户使用信息分析所述移动终端的用户是否异常;

c、如果所述移动终端的用户异常,则所述云端服务器向所述移动终端发送身份验证指令;以及

d、所述云端服务器接收所述移动终端根据所述身份验证指令返回的身份认证信息,并在所述身份认证信息正确时控制所述用户继续使用所述移动终端,否则所述云端服务器激活所述移动终端中的自锁程序对所述移动终端进行锁定。

2. 根据权利要求1所述的方法,其特征在于,所述用户使用信息包括位置信息、使用时间信息和用户使用习惯信息中的一种或多种。

3. 根据权利要求2所述的方法,其特征在于,所述步骤b具体包括:

b1、所述云端服务器根据获取的多个所述用户使用信息建立用户使用信息表;以及

b2、所述云端服务器监测所述用户使用信息表中的所述用户使用信息是否出现异常。

4. 根据权利要求3所述的方法,其特征在于,所述步骤b2具体包括:

所述云端服务器根据所述用户使用信息表中的所述位置信息获取所述用户的活动范围;

所述云端服务器判断所述用户使用信息表中的所述位置信息是否在所述活动范围之内;以及

如果不在所述活动范围之内,则所述云端服务器确定所述移动终端的所述用户异常。

5. 根据权利要求3所述的方法,其特征在于,所述步骤b2具体还包括:

所述云端服务器监测所述用户使用习惯信息是否出现异常。

6. 根据权利要求1-3任一项所述的方法,其特征在于,还包括:

所述云端服务器为每个所述用户使用信息设置权值;

所述云端服务器将异常的所述用户使用信息的权值进行求和;

所述云端服务器判断所述权值和是否大于预设阈值;以及

如果大于所述预设阈值,则所述云端服务器确定所述移动终端的所述用户异常。

7. 一种移动终端的身份验证的系统,其特征在于,包括:云端服务器和移动终端,其中,

所述云端服务器,用于按照预定的时间间隔获取所述移动终端的用户使用信息,并根据获取的多个所述用户使用信息分析所述移动终端的用户是否异常,以及在所述移动终端的用户异常时,向所述移动终端发送身份验证指令,并接收所述移动终端根据所述身份验证指令返回的身份认证信息,并在所述身份认证信息正确时控制所述用户继续使用所述移动终端,否则激活所述移动终端中的自锁程序对所述移动终端进行锁定。

8. 根据权利要求7所述的系统,其特征在于,所述用户使用信息包括位置信息、使用时间信息和用户使用习惯信息中的一种或多种。

9. 根据权利要求8所述的系统,其特征在于,所述云端服务器还用于:

根据获取的多个所述用户使用信息建立用户使用信息表,以及监测所述用户使用信息表中的所述用户使用信息是否出现异常。

10. 根据权利要求 9 所述的系统,其特征在于,所述云端服务器还用于:

根据所述用户使用信息表中的所述位置信息获取所述用户的活动范围,并判断所述用户使用信息表中的所述位置信息是否在所述活动范围之内,以及如果不在所述活动范围之内,则确定所述移动终端的所述用户异常。

11. 根据权利要求 9 所述的系统,其特征在于,所述云端服务器还用于:

监测所述用户使用习惯信息是否出现异常。

12. 根据权利要求 7-9 任一项所述的系统,其特征在于,所述云端服务器还用于:

为每个所述用户使用信息设置权值,并将异常的所述用户使用信息的权值进行求和,并判断所述权值和是否大于预设阈值,以及在大于所述预设阈值时,确定所述移动终端的所述用户异常。

移动终端的身份验证的方法和系统

技术领域

[0001] 本发明涉及移动互联网技术领域,特别涉及一种移动终端的身份验证的方法和系统。

背景技术

[0002] 目前,用户在使用移动终端时,一般设置移动终端的使用密码,用户输入正确的使用密码即可使用该移动终端。目前存在的问题是,移动终端针对用户没有任何特殊的识别和响应,无论什么用户,主要是正确的操作,都可使用该移动终端,例如输入正确的密码等,如果移动终端并未设置密码,或者其他用户知道使用密码或者密码被窃取,一旦移动终端丢失,可能被不法用户盗用。

发明内容

[0003] 本发明的目的旨在至少解决所述技术缺陷之一。

[0004] 为此,本发明的一个目的在于提出一种移动终端的身份验证的方法,该方法可根据用户的使用习惯对移动终端的用户进行身份认证,有效防止移动终端丢失或者被盗时的用户隐私泄露,保证信息安全,提升用户体验。

[0005] 本发明的第二个目的在于提出一种移动终端的身份验证的系统。

[0006] 为达到所述目的,本发明第一方面的实施例公开了一种移动终端的身份验证的方法,包括以下步骤:a、云端服务器按照预定的时间间隔获取移动终端的用户使用信息;b、所述云端服务器根据获取的多个所述用户使用信息分析所述移动终端的用户是否异常;c、如果所述移动终端的用户异常,则所述云端服务器向所述移动终端发送身份验证指令;以及d、所述云端服务器接收所述移动终端根据所述身份验证指令返回的身份认证信息,并在所述身份认证信息正确时控制所述用户继续使用所述移动终端,否则所述云端服务器激活所述移动终端中的自锁程序对所述移动终端进行锁定。

[0007] 根据本发明实施例的移动终端的身份验证的方法,云端服务器根据用户使用信息可以判断用户是否出现异常,并在出现异常时发送身份验证指令以对用户进行身份认证,可以根据用户的使用习惯对移动终端的用户进行身份认证,有效防止移动终端丢失或者被盗时的用户隐私泄露,保证信息安全,提升用户体验。

[0008] 为达到所述目的,本发明第二方面的实施例公开了一种移动终端的身份验证的系统,包括:云端服务器和移动终端,其中,所述云端服务器,用于按照预定的时间间隔获取所述移动终端的用户使用信息,并根据获取的多个所述用户使用信息分析所述移动终端的用户是否异常,以及在所述移动终端的用户异常时,向所述移动终端发送身份验证指令,并接收所述移动终端根据所述身份验证指令返回的身份认证信息,并在所述身份认证信息正确时控制所述用户继续使用所述移动终端,否则激活所述移动终端中的自锁程序对所述移动终端进行锁定。

[0009] 根据本发明实施例的移动终端的身份验证的系统,云端服务器根据用户使用信息

可以判断用户是否出现异常,并在出现异常时发送身份验证指令以对用户进行身份认证,可以根据用户的使用习惯对移动终端的用户进行身份认证,有效防止移动终端丢失或者被盗时的用户隐私泄露,保证信息安全,提升用户体验。

[0010] 本发明附加的方面和优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本发明的实践了解到。

附图说明

[0011] 本发明所述的和 / 或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解,其中:

[0012] 图 1 为根据本发明一个实施例的移动终端的身份验证的方法的流程图;

[0013] 图 2 为根据本发明另一个实施例的移动终端的身份验证的方法的流程图;以及

[0014] 图 3 为根据本发明一个实施例的移动终端的身份验证的系统的结构示意图。

具体实施方式

[0015] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,仅用于解释本发明,而不能解释为对本发明的限制。相反,本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0016] 在本发明的描述中,需要理解的是,术语“第一”、“第二”等仅用于描述目的,而不能理解为指示或暗示相对重要性。此外,在本发明的描述中,除非另有说明,“多个”的含义是两个或两个以上。

[0017] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为,表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分,并且本发明的优选实施方式的范围包括另外的实现,其中可以不按所示出或讨论的顺序,包括根据所涉及的功能按基本同时的方式或按相反的顺序,来执行功能,这应被本发明的实施例所属技术领域的技术人员所理解。

[0018] 下面参考附图描述根据本发明实施例的移动终端的身份验证的方法和系统。

[0019] 一种移动终端的身份验证的方法,包括以下步骤:a、云端服务器按照预定的时间间隔获取移动终端的用户使用信息;b、云端服务器根据获取的多个用户使用信息分析移动终端的用户是否异常;c、如果移动终端的用户异常,则云端服务器向移动终端发送身份验证指令;以及 d、云端服务器接收移动终端根据身份验证指令返回的身份认证信息,并在身份认证信息正确时控制用户继续使用移动终端,否则云端服务器激活移动终端中的自锁程序对移动终端进行锁定。

[0020] 图 1 为根据本发明一个实施例的移动终端的身份验证的方法的流程图。

[0021] 如图 1 所示,移动终端的身份验证的方法包括下述步骤。

[0022] 步骤 S101,云端服务器按照预定的时间间隔获取移动终端的用户使用信息。

[0023] 其中,预定的时间间隔可以是云端服务器或者移动终端自行设置的时间间隔。

[0024] 步骤 S102,云端服务器根据获取的多个用户使用信息分析移动终端的用户是否异

常。

[0025] 在本发明的一个实施例中,用户使用信息包括位置信息、使用时间信息和用户使用习惯信息中的一种或多种。例如,位置信息反映了用户经常活动的地理位置,如北京市西城区/通州区等,使用时间信息可以反映了用户的活动时间,如用户早上7点开机等,用户使用习惯信息可以包括多种习惯,如用户接听电话时喜欢开启免提等。

[0026] 步骤 S103,如果移动终端的用户异常,则云端服务器向移动终端发送身份验证指令。

[0027] 具体地,首先,云端服务器可以根据获取的多个用户使用信息进行统计分析获取移动终端用户的特征,一般用户使用移动终端时会有一定的规律,例如经常在北京市东城区活动,然后,云端服务器判断新获取的用户信息是否出现异常。

[0028] 步骤 S104,云端服务器接收移动终端根据身份验证指令返回的身份认证信息,并在身份认证信息正确时控制用户继续使用移动终端,否则云端服务器激活移动终端中的自锁程序对移动终端进行锁定。

[0029] 根据本发明实施例的移动终端的身份验证的方法,云端服务器根据用户使用信息可以判断用户是否出现异常,并在出现异常时发送身份验证指令以对用户进行身份认证,可以根据用户的使用习惯对移动终端的用户进行身份认证,有效防止移动终端丢失或者被盗时的用户隐私泄露,保证信息安全,提升用户体验。

[0030] 图2为根据本发明另一个实施例的移动终端的身份验证的方法的流程图。

[0031] 如图2所示,移动终端的身份验证的方法包括下述步骤。

[0032] 步骤 S201,云端服务器按照预定的时间间隔获取移动终端的用户使用信息。

[0033] 其中,预定的时间间隔可以是云端服务器或者移动终端自行设置的时间间隔。

[0034] 步骤 S202,云端服务器根据获取的多个用户使用信息建立用户使用信息表。

[0035] 在本发明的一个实施例中,用户使用信息包括位置信息、使用时间信息和用户使用习惯信息中的一种或多种。例如,位置信息反映了用户经常活动的地理位置,如北京市西城区/通州区等,使用时间信息可以反映了用户的活动时间,如用户早上7点开机等,用户使用习惯信息可以包括多种习惯,如用户接听电话时喜欢开启免提等。

[0036] 应当理解,用户使用信息表的建立也是持续的,根据预定的时间间隔对用户使用信息进行更新。

[0037] 步骤 S203,云端服务器监测用户使用信息表中的用户使用信息是否出现异常。

[0038] 其中,如果用户使用信息表中的用户使用信息出现异常,则移动终端的用户异常。

[0039] 步骤 S204,如果移动终端的用户异常,则云端服务器向移动终端发送身份验证指令。

[0040] 具体地,首先,云端服务器可以根据获取的多个用户使用信息进行统计分析获取移动终端用户的特征,一般用户使用移动终端时会有一定的规律,例如经常在北京市东城区活动,然后,云端服务器判断新获取的用户信息是否出现异常。

[0041] 步骤 S205,云端服务器接收移动终端根据身份验证指令返回的身份认证信息,并在身份认证信息正确时控制用户继续使用移动终端,否则云端服务器激活移动终端中的自锁程序对移动终端进行锁定。

[0042] 根据本发明实施例的移动终端的身份验证的方法,云端服务器通过建立用户使用

信息表对用户使用信息进行监测是否出现异常,提高了效率。

[0043] 根据用户使用信息表中的用户使用信息判断移动终端的用户是否异常,可以采用多种方法,下面进行详细说明。

[0044] 在本发明的一个实施例中,云端服务器根据用户使用信息表中的位置信息获取用户的活动范围;云端服务器判断用户使用信息表中的位置信息是否在不在活动范围之内;以及如果不在活动范围之内,则云端服务器确定移动终端的用户异常。例如,云端服务器根据用户使用信息表中的位置信息获取用户的活动范围为中国北京市西城区/通州区,当位置信息出现当前用户所处的位置为天津市时,则当前用户的异常。

[0045] 在本发明的一个实施例中,云端服务器监测用户使用习惯信息是否出现异常。例如,云端服务器根据用户使用信息表中的用户使用习惯信息显示该用户拨打电话时习惯于免提功能,次数在九成以上,云端服务器监测这种习惯在最近 10 次之内用户均没有采用免提,则判断用户异常。

[0046] 在本发明的一个实施例中,云端服务器为每个用户使用信息设置权值;云端服务器将异常的用户使用信息的权值进行求和;云端服务器判断权值和是否大于预设阈值;以及如果大于预设阈值,则云端服务器确定移动终端的用户异常。

[0047] 应当理解,以上的实施例仅为参考,还可以采用其他方法判断移动终端的用户是否异常。

[0048] 为了实现上述实施例,本发明还提出了一种移动终端的身份验证的系统。

[0049] 一种移动终端的身份验证的系统,包括:云端服务器和移动终端,其中,云端服务器,用于按照预定的时间间隔获取移动终端的用户使用信息,并根据获取的多个用户使用信息分析移动终端的用户是否异常,以及在移动终端的用户异常时,向移动终端发送身份验证指令,并接收移动终端根据身份验证指令返回的身份认证信息,并在身份认证信息正确时控制用户继续使用移动终端,否则激活移动终端中的自锁程序对移动终端进行锁定。

[0050] 图 3 为根据本发明一个实施例的移动终端的身份验证的系统的结构示意图。

[0051] 如图 3 所示,移动终端的身份验证的系统包括:云端服务器 10 和移动终端。

[0052] 具体地,云端服务器 10 用于按照预定的时间间隔获取移动终端 20 的用户使用信息,其中,预定的时间间隔可以是云端服务器 10 或者移动终端 20 自行设置的时间间隔,并根据获取的多个用户使用信息分析移动终端 20 的用户是否异常,以及在移动终端 20 的用户异常时,向移动终端 20 发送身份验证指令,并接收移动终端 20 根据身份验证指令返回的身份认证信息,并在身份认证信息正确时控制用户继续使用移动终端 20,否则激活移动终端 20 中的自锁程序对移动终端 20 进行锁定。

[0053] 在本发明的一个实施例中,用户使用信息包括位置信息、使用时间信息和用户使用习惯信息中的一种或多种。例如,位置信息反映了用户经常活动的地理位置,如北京市西城区/通州区等,使用时间信息可以反映了用户的活动时间,如用户早上 7 点开机等,用户使用习惯信息可以包括多种习惯,如用户接听电话时喜欢开启免提等。

[0054] 更具体地,首先,云端服务器 10 可以根据获取的多个用户使用信息进行统计分析获取移动终端 20 用户的特征,一般用户使用移动终端 20 时会有一定的规律,例如经常在北京市东城区活动,然后,云端服务器 10 判断新获取的用户信息是否出现异常。

[0055] 根据本发明实施例的移动终端的身份验证的系统,云端服务器根据用户使用信息

可以判断用户是否出现异常,并在出现异常时发送身份验证指令以对用户进行身份认证,可以根据用户的使用习惯对移动终端的用户进行身份认证,有效防止移动终端丢失或者被盗时的用户隐私泄露,保证信息安全,提升用户体验。

[0056] 在本发明的一个实施例中,云端服务器 10 还用于:根据获取的多个用户使用信息建立用户使用信息表,以及监测用户使用信息表中的用户使用信息是否出现异常。其中,如果用户使用信息表中的用户使用信息出现异常,则移动终端 20 的用户异常。

[0057] 云端服务器 10 根据用户使用信息表中的用户使用信息判断移动终端的用户是否异常,可以采用多种方法,下面进行详细说明。

[0058] 在本发明的一个实施例中,云端服务器 10 还用于:根据用户使用信息表中的位置信息获取用户的活动范围,并判断用户使用信息表中的位置信息是否在活动范围之内,以及如果不在活动范围之内,则确定移动终端 20 的用户异常。例如,云端服务器 10 根据用户使用信息表中的位置信息获取用户的活动范围为中国北京市西城区 / 通州区,当位置信息出现当前用户所处的位置为天津市时,则当前用户的异常。

[0059] 在本发明的一个实施例中,云端服务器 10 还用于:监测用户使用习惯信息是否出现异常。例如,云端服务器 10 根据用户使用信息表中的用户使用习惯信息显示该用户拨打电话时习惯于免提功能,次数在九成以上,云端服务器 10 监测这种习惯在最近 10 次之内用户均没有采用免提,则判断用户异常。

[0060] 在本发明的一个实施例中,云端服务器 10 还用于:为每个用户使用信息设置权值,并将异常的用户使用信息的权值进行求和,并判断权值和是否大于预设阈值,以及在大于预设阈值时,确定移动终端的所述用户异常。

[0061] 应当理解,以上的实施例仅为参考,还可以采用其他方法判断移动终端的用户是否异常。

[0062] 应当理解,在本发明的实施例中,移动终端可以是手机、平板电脑、个人数字助理、电子书等具有各种操作系统的硬件设备。

[0063] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对所述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何一个或多个实施例或示例中以合适的方式结合。

[0064] 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限定。

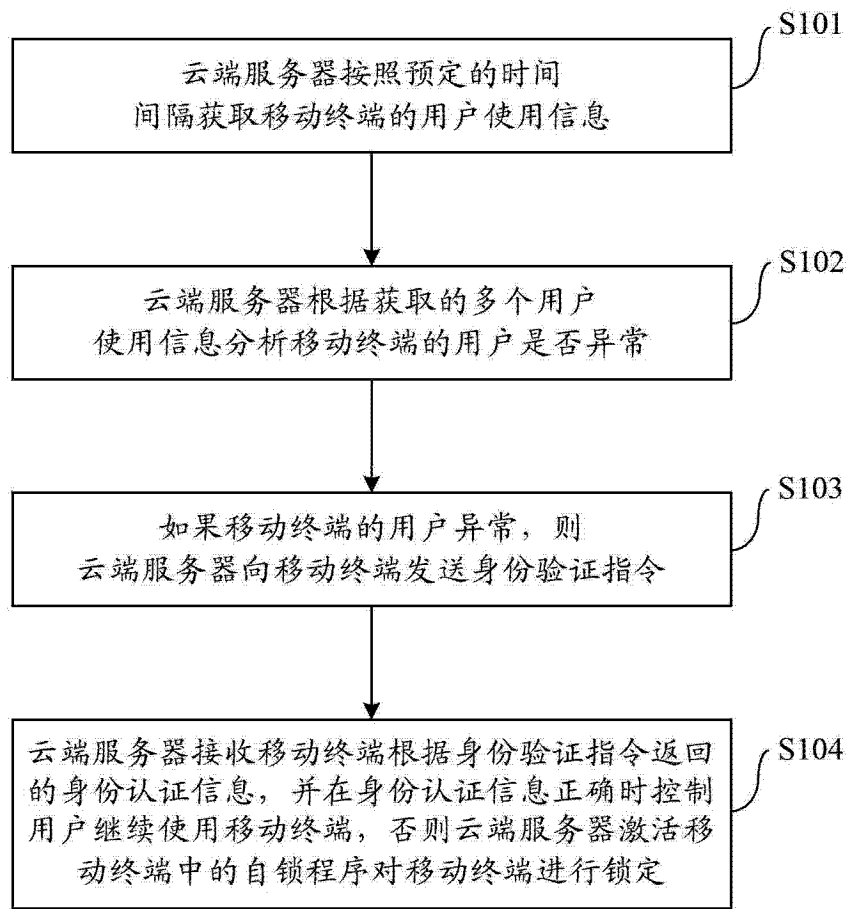


图 1

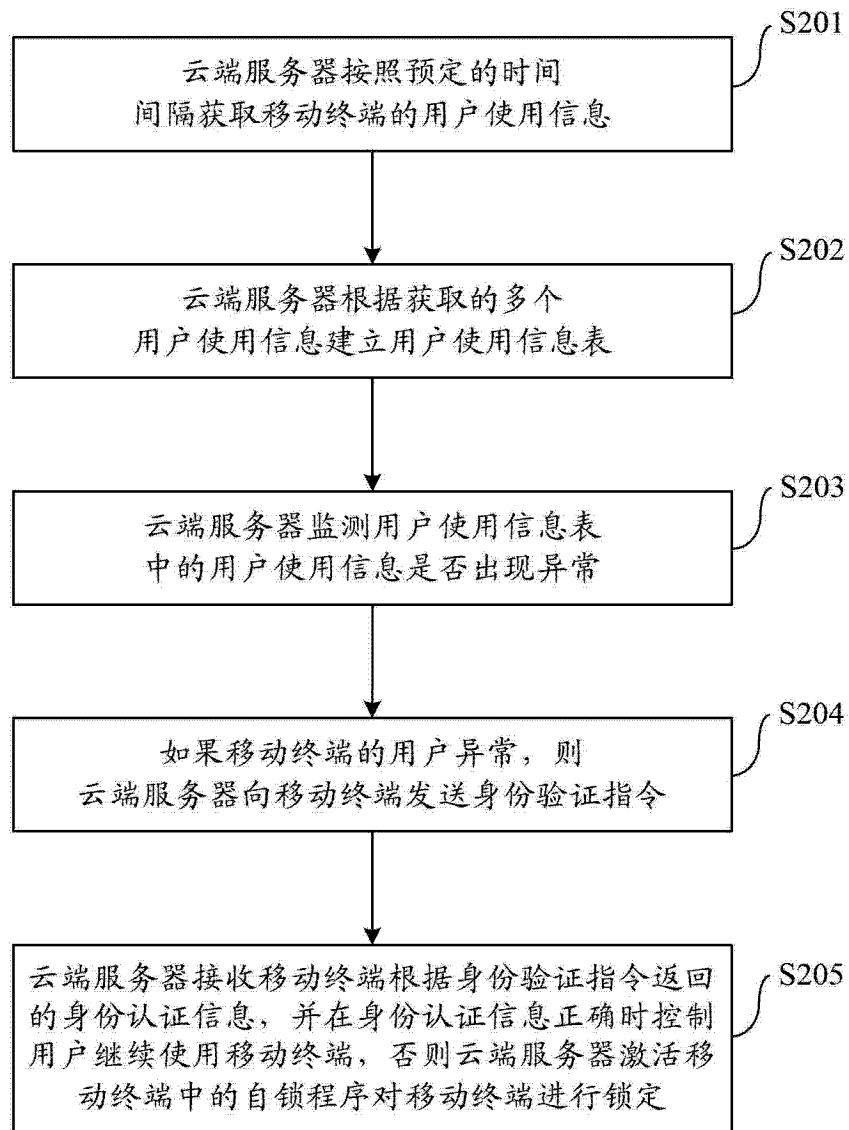


图 2

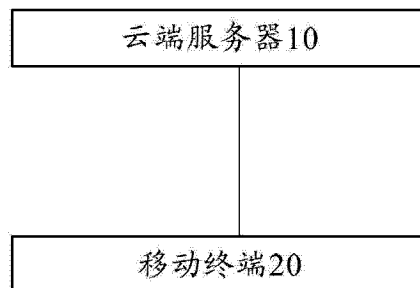


图 3