(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103188213 B
(45)授权公告日 2016.04.06

(21)申请号 201110446549.X

(22)申请日 2011.12.28

(73)专利权人 宇龙计算机通信科技(深圳)有限公司
地址 518040 广东省深圳市车公庙天安数码城创新科技广场B座8楼

(72)发明人 洪济宇

(74)专利代理机构 北京友联知识产权代理事务所(普通合伙) 11343
代理人 尚志峰 汪海屏

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 102215229 A,2011.10.12,
CN 102215229 A,2011.10.12,
CN 102253858 A,2011.11.23,
US 2008/0072257 A1,2008.03.20,
CN 102200922 A,2011.09.28,
CN 101505343 A,2009.08.12,

审查员 张承承

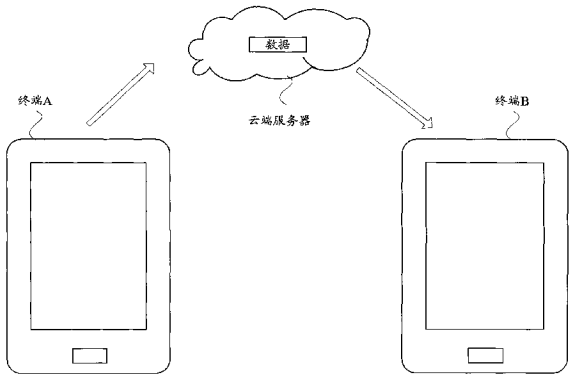
权利要求书1页 说明书5页 附图2页

(54)发明名称

服务器和网络交互控制方法

(57)摘要

本发明提供一种服务器和一种网络交互控制方法,其中,服务器包括:数据获取模块,在不同设备之间需进行数据传输时,获取发送端发出的数据;分析控制模块,根据预定规则对所述数据进行分析,并根据分析结果判断是否将所述数据发送到接收端。在该技术方案中,用户可以灵活设置规则,来有效控制哪些数据可以上传或下载,哪些数据不可以上传或下载,同时满足用户传输数据的需要以及用户数据的安全。该服务器可以是云端服务器。



CN 103188213 B

1. 一种服务器，其特征在于，包括：

数据获取模块，在不同设备之间需进行数据传输时，获取发送端发出的数据；

分析控制模块，根据预定规则对所述数据进行分析，并根据分析结果判断是否将所述数据发送到接收端；

信息提供模块，查询出所述发送端中发送所述数据和/或所述接收端中接收所述数据的应用程序，并将来自不同终端的所述应用程序的相关信息，发送给所述发送端和/或所述接收端。

2. 根据权利要求 1 所述的服务器，其特征在于，所述分析控制模块分析所述数据是否为所述发送端中特定的关键数据，和/或是否为影响所述接收端正常使用的危害性数据，并根据分析结果判断是否将所述数据发送到所述接收端。

3. 根据权利要求 2 所述的服务器，其特征在于，所述分析控制模块在所述数据是所述关键数据和/或所述危害性数据时，向所述发送端和/或所述接收端请求身份证明，并在接收到所述发送端和/或所述接收端的身份证明时，将所述数据发送所述接收端。

4. 根据权利要求 1 所述的服务器，其特征在于，所述应用程序的相关信息包括：

所述应用程序进行特定操作的记录、所述应用程序的权限设置、所述应用程序的相关评论。

5. 一种网络交互控制方法，其特征在于，包括：

步骤 202，在不同设备之间需进行数据传输时，获取发送端发出的数据；

步骤 204，根据预定规则对所述数据进行分析，并根据分析结果判断是否将所述数据发送到接收端；

步骤 206，查询出所述发送端中发送所述数据和/或所述接收端中接收所述数据的应用程序，并将来自不同终端的所述应用程序的相关信息，发送给所述发送端和/或所述接收端。

6. 根据权利要求 5 所述的网络交互控制方法，其特征在于，所述步骤 204 具体包括：

分析所述数据是否为所述发送端中特定的关键数据，和/或是否为影响所述接收端正常使用的危害性数据，并根据分析结果判断是否将所述数据发送到所述接收端。

7. 根据权利要求 6 所述的网络交互控制方法，其特征在于，所述步骤 204 还包括：

在所述数据是所述关键数据和/或所述危害性数据时，向所述发送端和/或所述接收端请求身份证明，并在接收到所述发送端和/或所述接收端的身份证明时，将所述数据发送所述接收端。

8. 根据权利要求 5 所述的网络交互控制方法，其特征在于，所述应用程序的相关信息包括：

所述应用程序进行特定操作的记录、所述应用程序的权限设置、所述应用程序的相关评论。

服务器和网络交互控制方法

技术领域

[0001] 本发明涉及移动通信领域，具体而言，涉及一种服务器和一种网络交互控制方法。

背景技术

[0002] 目前的手机系统中，大多提供了对应用的权限控制。以 Android 系统为例，现有控制应用访问数据网络的方法一般仅仅是列出具有访问网络权限的应用列表，供用户选择是否禁止应用访问数据网络。通过 iptables 组件（用于增删改权限规则）向 netfilter 组件（包含权限规则）写入权限规则，来达到控制上网的目的。

[0003] 目前，手机仅仅能够根据权限列表来列出具有访问网络权限的应用但对于此应用具体信息如是否访问联系人，是否自动读 / 发短信等没有其他描述，对于应用具体上传 / 下载信息内容也不清楚。

[0004] 而用户自身对其不了解的应用，往往无法知道是否应该禁止其访问网络，而且，用户允许访问网络的某些应用在上传某些特定类型的关键数据时，如联系人、短信等，无法对这些数据进行分析，用户也无法对传输过程进行阻止，这样会给用户造成不小的损失。

[0005] 因此，需要一种新的针对手机终端访问网络的控制方案，能够保证手机终端在访问网络的过程中，不会上传手机中的关键数据，也不会下载影响手机使用的危害性数据，同时，需要自动获取不同应用程序的相关信息，以用于判断是否允许该应用程序访问网络。

发明内容

[0006] 本发明所要解决的技术问题在于，提供一种新的针对手机终端访问网络的控制方案，能够保证手机终端在访问网络的过程中，不会上传手机中的关键数据，也不会下载影响手机使用的危害性数据，同时，需要自动获取不同应用程序的相关信息，以用于判断是否允许该应用程序访问网络。

[0007] 有鉴于此，本发明提供一种服务器，包括：数据获取模块，在不同设备之间需进行数据传输时，获取发送端发出的数据；分析控制模块，根据预定规则对所述数据进行分析，并根据分析结果判断是否将所述数据发送到接收端。在该技术方案中，用户可以灵活设置规则，来有效控制哪些数据可以上传或下载，哪些数据不可以上传或下载，同时满足用户传输数据的需要以及用户数据的安全。该服务器可以是云端服务器。

[0008] 在上述技术方案中，优选地，所述分析控制模块分析所述数据是否为所述发送端中特定的关键数据，和 / 或是否为影响所述接收端正常使用的危害性数据，并根据分析结果判断是否将所述数据发送到所述接收端。在该技术方案中，保证了用户既不会将如通讯录、短信等关键数据提供给他人，也不会下载一些例如恶意程序的危害性数据。

[0009] 在上述技术方案中，优选地，所述分析控制模块在所述数据是所述关键数据和 / 或所述危害性数据时，向所述发送端和 / 或所述接收端请求身份证明，并在接收到所述发送端和所 / 或所述接收端的身份证明时，将所述数据发送所述接收端。在该技术方案中，可以准确地判断出上传或下载数据的操作，是否根据用户本人的意愿发出，既保证了信息传

输的安全，又不会妨碍用户传输数据的需要。

[0010] 在上述技术方案中，优选地，还包括：信息提供模块，查询出所述发送端中发送所述数据和/或所述接收端中接受所述数据的应用程序，并将来自不同终端的所述应用程序的相关信息，发送给所述发送端和/或所述接收端。在该技术方案中，可以收集不同应用程序的相关信息，以供用户参考。

[0011] 在上述技术方案中，优选地，所述应用程序的相关信息包括：所述应用程序进行特定操作的记录、所述应用程序的权限设置、所述应用程序的相关评论。在该技术方案中，特定操作可以是访问关键数据的操作，权限设置可以包括访问网络的权限设置，相关评论可以是不同用户对应用程序的各种评论。

[0012] 本发明还提供一种网络交互控制方法，包括：步骤 202，在不同设备之间需进行数据传输时，获取发送端发出的数据；步骤 204，根据预定规则对所述数据进行分析，并根据分析结果判断是否将所述数据发送到接收端。在该技术方案中，用户可以灵活设置规则，来有效控制哪些数据可以上传或下载，哪些数据不可以上传或下载，同时满足用户传输数据的需要以及用户数据的安全。

[0013] 在上述技术方案中，优选地，所述步骤 204 具体包括：分析所述数据是否为所述发送端中特定的关键数据，和/或是否为影响所述接收端正常使用的危害性数据，并根据分析结果判断是否将所述数据发送到所述接收端。在该技术方案中，保证了用户既不会将如通讯录、短信等关键数据提供给他人，也不会下载一些例如恶意程序的危害性数据。

[0014] 在上述技术方案中，优选地，所述步骤 204 还包括：在所述数据是所述关键数据和/或所述危害性数据时，向所述发送端和/或所述接收端请求身份证明，并在接收到所述发送端和所/或所述接收端的身份证明时，将所述数据发送所述接收端。在该技术方案中，可以准确地判断出上传或下载数据的操作，是否根据用户本人的意愿发出，既保证了信息传输的安全，又不会妨碍用户传输数据的需要。

[0015] 在上述技术方案中，优选地，还包括：查询出所述发送端中发送所述数据和/或所述接收端中接受所述数据的应用程序，并将来自不同终端的所述应用程序的相关信息，发送给所述发送端和/或所述接收端。在该技术方案中，可以收集不同应用程序的相关信息，以供用户参考。

[0016] 在上述技术方案中，优选地，所述应用程序的相关信息包括：所述应用程序进行特定操作的记录、所述应用程序的权限设置、所述应用程序的相关评论。在该技术方案中，特定操作可以是访问关键数据的操作，权限设置可以包括访问网络的权限设置，相关评论可以是不同用户对应用程序的各种评论。

[0017] 通过以上技术方案，可以实现一种服务器和一种网络交互控制方法，当应用程序上传与下载数据时，首先在云端服务器进行判断分析，防止应用程序上传用户的关键数据或下载会影响用户正常使用手机的数据，同时向用户提供了手机安装的应用程序的使用信息，根据不同用户对于应用程序访问网络的控制设置、应用程序访问手机关键数据的次数，让用户更好的判断是否禁止应用程序访问网络。

附图说明

[0018] 图 1 是根据本发明的一个实施例的服务器的框图；

[0019] 图 2 是根据本发明的一个实施例的网络交互控制方法的流程图；

[0020] 图 3 是根据本发明的一个实施例的网络交互控制方法的示意图。

具体实施方式

[0021] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。

[0022] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明并不限于下面公开的具体实施例的限制。

[0023] 图 1 是根据本发明的一个实施例的服务器的框图。

[0024] 如图 1 所示，本发明提供一种服务器 100，包括：数据获取模块 102，在不同设备之间需进行数据传输时，获取发送端发出的数据；分析控制模块 104，根据预定规则对所述数据进行分析，并根据分析结果判断是否将所述数据发送到接收端。在该技术方案中，用户可以灵活设置规则，来有效控制哪些数据可以上传或下载，哪些数据不可以上传或下载，同时满足用户传输数据的需要以及用户数据的安全。该服务器可以是云端服务器。

[0025] 在上述技术方案中，所述分析控制模块 104 分析所述数据是否为所述发送端中特定的关键数据，和 / 或是否为影响所述接收端正常使用的危害性数据，并根据分析结果判断是否将所述数据发送到所述接收端。在该技术方案中，保证了用户既不会将如通讯录、短信等关键数据提供给他人，也不会下载一些例如恶意程序的危害性数据。

[0026] 在上述技术方案中，所述分析控制模块 104 在所述数据是所述关键数据和 / 或所述危害性数据时，向所述发送端和 / 或所述接收端请求身份证明，并在接收到所述发送端和所 / 或所述接收端的身份证明时，将所述数据发送所述接收端。在该技术方案中，可以准确地判断出上传或下载数据的操作，是否根据用户本人的意愿发出，既保证了信息传输的安全，又不会妨碍用户传输数据的需要。

[0027] 在上述技术方案中，还包括：信息提供模块 106，查询出所述发送端中发送所述数据和 / 或所述接收端中接受所述数据的应用程序，并将来自不同终端的所述应用程序的相关信息，发送给所述发送端和 / 或所述接收端。在该技术方案中，可以收集不同应用程序的相关信息，以供用户参考。

[0028] 在上述技术方案中，所述应用程序的相关信息包括：所述应用程序进行特定操作的记录、所述应用程序的权限设置、所述应用程序的相关评论。在该技术方案中，特定操作可以是访问关键数据的操作，权限设置可以包括访问网络的权限设置，相关评论可以是不同用户对应用程序的各种评论。

[0029] 图 2 是根据本发明的一个实施例的网络交互控制方法的流程图。

[0030] 如图 2 所示，本发明还提供一种网络交互控制方法，包括：步骤 202，在不同设备之间需进行数据传输时，获取发送端发出的数据；步骤 204，根据预定规则对所述数据进行分析，并根据分析结果判断是否将所述数据发送到接收端。在该技术方案中，用户可以灵活设置规则，来有效控制哪些数据可以上传或下载，哪些数据不可以上传或下载，同时满足用户传输数据的需要以及用户数据的安全。

[0031] 在上述技术方案中，所述步骤 204 具体包括：分析所述数据是否为所述发送端中

特定的关键数据，和 / 或是否为影响所述接收端正常使用的危害性数据，并根据分析结果判断是否将所述数据发送到所述接收端。在该技术方案中，保证了用户既不会将如通讯录、短信等关键数据提供给他人，也不会下载一些例如恶意程序的危害性数据。

[0032] 在上述技术方案中，所述步骤 204 还包括 ：在所述数据是所述关键数据和 / 或所述危害性数据时，向所述发送端和 / 或所述接收端请求身份证明，并在接收到所述发送端和所 / 或所述接收端的身份证明时，将所述数据发送所述接收端。在该技术方案中，可以准确地判断出上传或下载数据的操作，是否根据用户本人的意愿发出，既保证了信息传输的安全，又不会妨碍用户传输数据的需要。

[0033] 在上述技术方案中，还包括 ：查询出所述发送端中发送所述数据和 / 或所述接收端中接受所述数据的应用程序，并将来自不同终端的所述应用程序的相关信息，发送给所述发送端和 / 或所述接收端。在该技术方案中，可以收集不同应用程序的相关信息，以供用户参考。

[0034] 在上述技术方案中，所述应用程序的相关信息包括 ：所述应用程序进行特定操作的记录、所述应用程序的权限设置、所述应用程序的相关评论。在该技术方案中，特定操作可以是访问关键数据的操作，权限设置可以包括访问网络的权限设置，相关评论可以是不同用户对应用程序的各种评论。

[0035] 在本发明的一个实施例中，通过云端服务器的统计与分析，可以防止用户的关键数据被上传到网络上，并能防止用户终端自动下载影响手机终端正常使用的危害性数据，如图 3 所示，本方案实现步骤如下 ：

[0036] 一、不同用户的终端获取唯一身份证明，此处，假设用户终端包括终端 A 和终端 B。

[0037] 二、(1) 终端 A 或终端 B 的用户禁止 / 允许应用程序访问网络时，当该设置保存超过一天，终端 A 或终端 B 将此应用的唯一标示发送到云端服务器进行统计 ；

[0038] (2) 云端服务器根据包括终端 A 和终端 B 的所有终端发送的信息统计某应用程序的允许 / 禁止访问网络的比例与使用人数等信息，并将这些信息显示到终端 A 和终端 B 中 ；

[0039] (3) 终端 A 和终端 B 的用户可以评论此应用，发送到云端服务器，云端服务器集中评论信息后，提供给终端 A 和终端 B，供用户查看。

[0040] 三、(1) 终端 A 或终端 B 中的某个应用程序访问联系人、发送短信、访问短信、访问日历等关键数据时，终端 A 或终端 B 记录下访问次数并发送给云端服务器 ；

[0041] (2) 云端服务器根据所有用户终端发送的数据，统计该应用程序平均每天在每台终端上访问关键数据的次数，并提供给终端 A 和终端 B 的用户查看。

[0042] 四、(1) 当终端 A(终端 B 的情况类似) 中的应用程序发送数据时，首先将数据发送到云端服务器，云端服务器检查该数据是否为终端 A 的关键数据，如果为关键数据，则给终端 A 发送消息，提醒用户正在上传关键数据，用户只有正确输入唯一身份证明时，云端服务器才能继续上传数据到数据接收端，否则不上传数据 ；

[0043] (2) 当终端 B(终端 A 的情况类似) 中的应用程序要接收数据时，云端服务器先接收数据，分析判断这些数据是否会影响到终端 B 正常工作，并且发送消息给终端 B，提醒用户是否接收数据，用户只有正确输入唯一身份证明时，云端才能继续把接收数据发送到终端 B，否则不转发数据。

[0044] 综上所述，通过以上技术方案，可以实现一种服务器和一种网络交互控制方法，设

计了根据云端服务器数据分析提供给用户访问网络应用详细信息，供用户选择是否允许其访问网络，选择禁止应用访问网络时，提供给云端服务器该应用程序的信息，云端服务器统计所有用户提供的数据，由此可以查看多少使用该应用程序的用户禁止这个应用访问网络，并供其他用户参考；可以对应用程序进行评论，供安装该应用程序的用户查看；对应用程序访问手机其他信息时，记录下访问次数，并提供给云端服务器，统计所有用户提供的数据，供用户查看该应用程序每天平均访问其他数据的次数；当应用程序上传数据时，先传送到云端服务器进行分析，如果是关键数据，给手机端发送警告，用户提供唯一身份证明才能上传，当应用程序下载数据时，如果数据会危害到用户，同样发送警告，用户提供唯一身份证明才能下载。

[0045] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

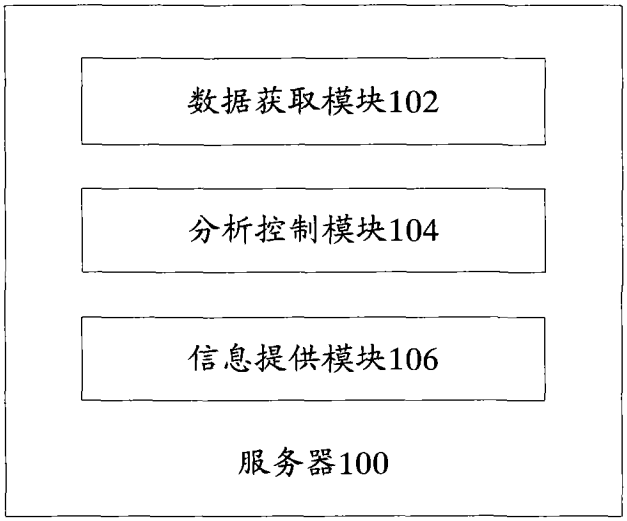

数据获取模块102
分析控制模块104
信息提供模块106
服务器100

图 1

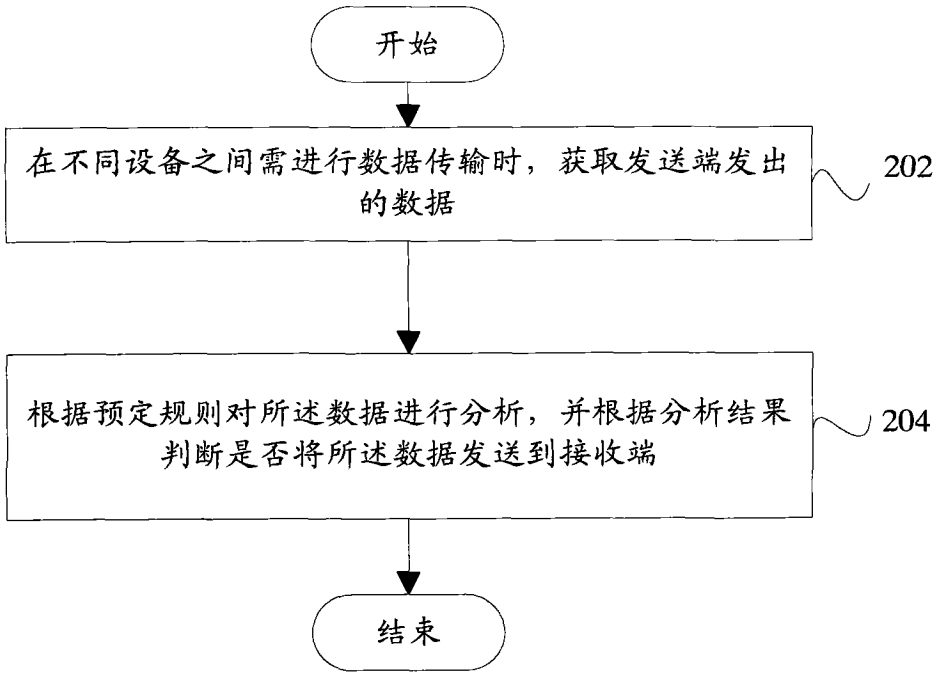

开始
在不同设备之间需进行数据传输时，获取发送端发出的数据
202
根据预定规则对所述数据进行分析，并根据分析结果判断是否将所述数据发送到接收端
204
结束

图 2

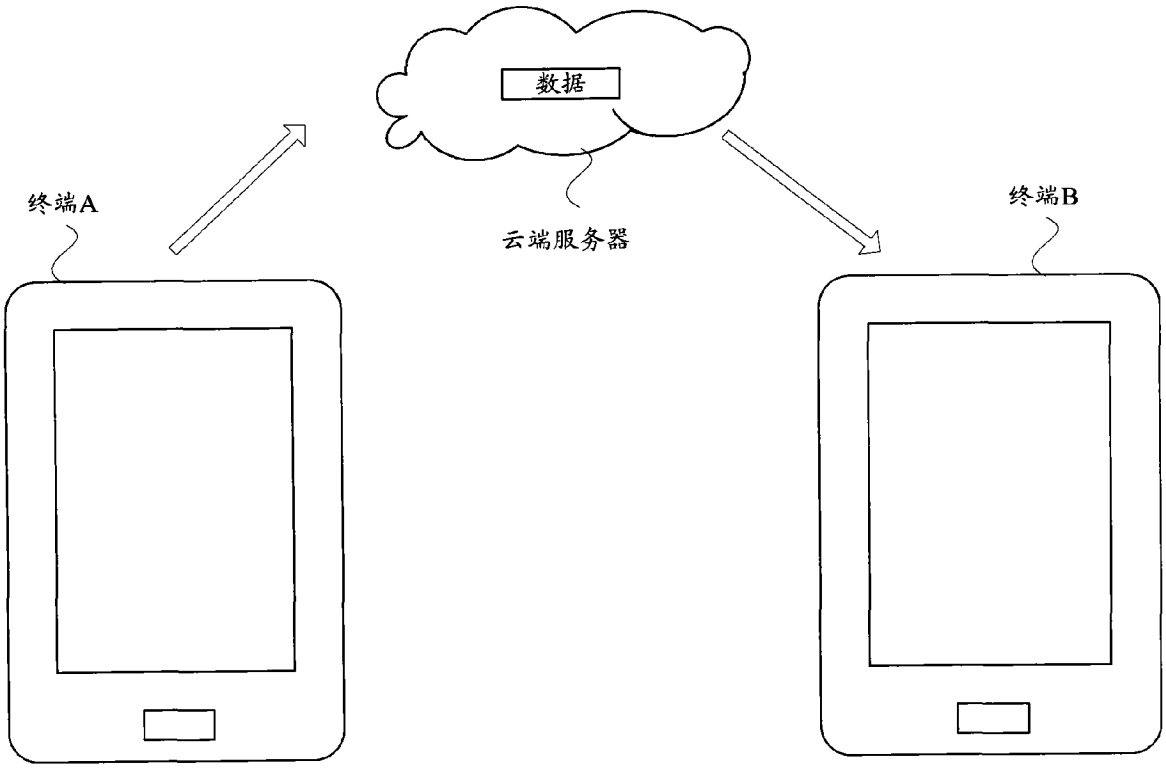


图 3