(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 106412909 B
(45)授权公告日 2019.09.27

(21)申请号 201610913492.2

(22)申请日 2016.10.19

(65)同一申请的已公布的文献号
申请公布号 CN 106412909 A

(43)申请公布日 2017.02.15

(73)专利权人 广东欧珀移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号

(72)发明人 周璇

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04W 12/08(2009.01)
H04W 76/11(2018.01)
H04W 76/14(2018.01)

(56)对比文件
CN 103957103 A,2014.07.30,
CN 102823190 A,2012.12.12,
CN 104320412 A,2015.01.28,
CN 102130904 A,2011.07.20,
CN 103391273 A,2013.11.13,
CN 103477666 A,2013.12.25,
CN 103813334 A,2014.05.21,
CN 102201845 A,2011.09.28,

审查员 马兴婕

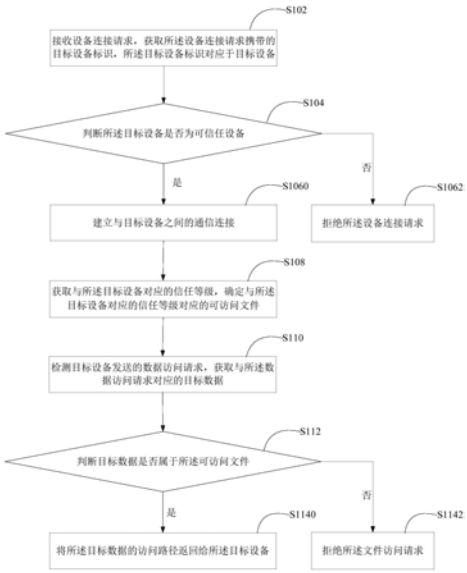
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种设备连接的方法及装置

(57)摘要

本发明实施例公开了一种设备连接的方法及装置,其中所述方法包括:接收设备连接请求,获取所述设备连接请求携带的目标设备标识,所述目标设备标识对应于目标设备;判断所述目标设备是否为可信任设备,若为可信任设备,则建立与目标设备之间的通信连接;获取与所述目标设备对应的信任等级,确定与所述目标设备对应的信任等级对应的可访问文件;检测目标设备发送的数据访问请求,获取与所述数据访问请求对应的目标数据;判断目标数据是否属于所述可访问文件,若所述目标数据属于所述可访问文件,则将所述目标数据的访问路径返回给所述目标设备,否则,拒绝所述文件访问请求。采用本发明实施例,可提高设备连接的安全性。



CN 106412909 B

1.一种设备连接的方法,其特征在于,包括:

接收设备连接请求,获取所述设备连接请求携带的目标设备标识,所述目标设备标识对应于目标设备;

判断所述目标设备是否为可信任设备,若为可信任设备,则建立与目标设备之间的通信连接,其中,所述通信连接为蓝牙连接或WiFi连接;

获取与所述目标设备对应的信任等级,确定与所述目标设备对应的信任等级对应的可访问文件;

检测目标设备发送的数据访问请求,获取与所述数据访问请求对应的目标数据;

判断目标数据是否属于所述可访问文件,若所述目标数据属于所述可访问文件,则将所述目标数据的访问路径返回给所述目标设备,否则,拒绝所述文件访问请求;

在设备连接建立成功后,检测与目标设备对应数据传输流量,在所述数据传输流量大于预设的流量阈值的情况下,暂停与所述目标设备之间的数据传输;

其中,所述获取与所述目标设备对应的信任等级的步骤还包括:

获取与目标设备对应的历史连接记录,所述历史连接记录包括历史连接次数和/或历史连接时长;

根据预设的信任等级计算公式,以所述历史连接次数和/或历史连接时长为自变量计算与所述目标设备对应的信任等级,包括:每增加一次历史连接次数,计1分,连接时长每增加1h,计1分,将所有的计分的总和确定为最终的信用分数,并根据最终的信用分数确定对应的信任等级。

2.根据权利要求1所述的设备连接的方法,其特征在于,所述判断所述目标设备是否为可信任设备的步骤还包括:

在预设的可信任设备列表中查找与所述目标设备标识匹配的设备标识,若查找到,则判定所述目标设备为可信任设备。

3.根据权利要求1至2任一所述的设备连接的方法,其特征在于,所述接收设备连接请求的步骤之后还包括:

接收所述目标设备发送的密码,所述密码由所述目标设备根据检测到的在目标设备上输入的字符串生成;

判断所述密码是否与预设值匹配,若是,则执行所述判断所述目标设备是否为可信任设备的步骤,否则,拒绝所述设备连接请求。

4.根据权利要求2所述的设备连接的方法,其特征在于,所述判断所述目标设备是否为可信任设备的步骤之后还包括:

在所述目标设备不为可信任设备时,接收用户输入的设备添加指令;

根据所述设备添加指令,将所述目标设备标识添加至所述预设的可信任设备列表。

5.根据权利要求1所述的设备连接的方法,其特征在于,所述检测与目标设备对应数据传输流量,在所述数据传输流量大于预设的流量阈值的情况下,暂停与所述目标设备之间的数据传输之后,所述方法还包括:

生成提示消息进行展示;

检测针对所述提示消息输入的操作指令,所述操作指令包括数据传输继续指令和设备连接断开指令;

在所述操作指令为数据传输继续指令时，移除对与所述数据传输的暂停状态；

在所述操作指令为设备连接断开指令时，断开与所述目标设备之间的通信连接。

6.一种设备连接的装置，其特征在于，包括：

设备连接请求接收模块，用于接收设备连接请求，获取所述设备连接请求携带的目标设备标识，所述目标设备标识对应于目标设备；

通信连接建立模块，用于判断所述目标设备是否为可信任设备，在所述目标设备为可信任设备时，建立与目标设备之间的通信连接，其中，所述通信连接为蓝牙连接或WiFi连接；

信任等级确定模块，用于获取与所述目标设备对应的信任等级，确定与所述目标设备对应的信任等级对应的可访问文件；

数据访问请求检测模块，用于检测目标设备发送的数据访问请求，获取与所述数据访问请求对应的目标数据；

数据访问请求响应模块，用于判断目标数据是否属于所述可访问文件，在所述目标数据属于所述可访问文件时，将所述目标数据的访问路径返回给所述目标设备，在所述目标数据不属于所述可访问文件时，拒绝所述文件访问请求；

数据传输流量控制模块，用于检测与目标设备对应数据传输流量，在所述数据传输流量大于预设的流量阈值的情况下，暂停与所述目标设备之间的数据传输；

其中，所述信任等级确定模块还用于获取与目标设备对应的历史连接记录，所述历史连接记录包括历史连接次数和/或历史连接时长；根据预设的信任等级计算公式，以所述历史连接次数和/或历史连接时长为自变量计算与所述目标设备对应的信任等级，包括：每增加一次历史连接次数，计1分，连接时长每增加1h，计1分，将所有的计分的总和确定为最终的信用分数，并根据最终的信用分数确定对应的信任等级。

7.根据权利要求6所述的设备连接的装置，其特征在于，所述通信连接建立模块还用于在预设的可信任设备列表中查找与所述目标设备标识匹配的设备标识，在查找到时，判定所述目标设备为可信任设备。

8.根据权利要求6至7任一所述的设备连接的装置，其特征在于，所述装置还包括密码验证模块，用于接收所述目标设备发送的密码，所述密码由所述目标设备根据检测到的在目标设备上输入的字符串生成；判断所述密码是否与预设值匹配，若是，则触发通信连接建立模块执行判断所述目标设备是否为可信任设备的功能，否则，拒绝所述设备连接请求。

9.根据权利要求7所述的设备连接的装置，其特征在于，所述通信连接建立模块还用于在所述目标设备不为可信任设备时，接收用户输入的设备添加指令；根据所述设备添加指令，将所述目标设备标识添加至所述预设的可信任设备列表。

10.根据权利要求6所述的设备连接的装置，其特征在于，所述数据传输流量控制模块还用于生成提示消息进行展示；检测针对所述提示消息输入的操作指令，所述操作指令包括数据传输继续指令和设备连接断开指令；在所述操作指令为数据传输继续指令时，移除对与所述数据传输的暂停状态；在所述操作指令为设备连接断开指令时，断开与所述目标设备之间的通信连接。

11.一种计算机可读存储介质，其特征在于，所述计算机可存储介质中存储有程序指令，所述程序指令用于供计算机调用后执行如权利要求1-5任一项所述的方法。

一种设备连接的方法及装置

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种设备连接的方法及装置。

背景技术

[0002] 随着终端技术的发展，在智能手机、蓝牙耳机等多种设备上均集成了蓝牙功能，两个具备蓝牙功能的设备或终端可以在建立了相关之间的蓝牙连接之后进行数据交互，因为通过蓝牙进行数据的传输可以在短距离类实现数据的传输，并且具有延迟时间段、连接稳定性强的有点。

[0003] 一般来讲，两个具备蓝牙功能的设备或终端在建立相互之间的连接时，例如在两个智能手机在建立蓝牙连接时，需要互相之间匹配PIN码或者输入预设的密码，而一般来讲，PIN码或者预设密码都是较为简单的4位数字，例如，“0000”，或者，有的终端采取的是无验证的连接方式。因此在两个终端建立了蓝牙连接之后即可进行数据的传输，若采取无验证的方式则可能导致数据遭到窃听或盗取，进一步的，若在连接时采用上述PIN码的验证方式，因为容易被破解也存在安全性的问题。

发明内容

[0004] 本发明实施例提出了一种设备连接的方法，可以解决蓝牙终端之间的连接方式容易导致数据被窃取存在安全性不足的技术问题。

[0005] 一种设备连接的方法，包括：

[0006] 接收设备连接请求，获取所述设备连接请求携带的目标设备标识，所述目标设备标识对应于目标设备；

[0007] 判断所述目标设备是否为可信任设备，若为可信任设备，则建立与目标设备之间的通信连接；

[0008] 获取与所述目标设备对应的信任等级，确定与所述目标设备对应的信任等级对应的可访问文件；

[0009] 检测目标设备发送的数据访问请求，获取与所述数据访问请求对应的目标数据；

[0010] 判断目标数据是否属于所述可访问文件，若所述目标数据属于所述可访问文件，则将所述目标数据的访问路径返回给所述目标设备，否则，拒绝所述文件访问请求。

[0011] 可选的，在其中一个实施例中，所述获取与所述目标设备对应的信任等级的步骤还包括：

[0012] 获取与目标设备对应的历史连接记录，所述历史连接记录包括历史连接次数和/或历史连接时长；

[0013] 根据预设的信任等级计算公式，以所述历史连接次数和/或历史连接时长为自变量计算与所述目标设备对应的信任等级。

[0014] 可选的，在其中一个实施例中，所述判断所述目标设备是否为可信任设备的步骤还包括：

[0015] 在预设的可信任设备列表中查找与所述目标设备标识匹配的设备标识，若查找到，则判定所述目标设备为可信任设备。

[0016] 可选的，在其中一个实施例中，所述接收设备连接请求的步骤之后还包括：

[0017] 接收所述目标设备发送的密码，所述密码由所述目标设备根据检测到的在目标设备上输入的字符串生成；

[0018] 判断所述密码是否与预设值匹配，若是，则执行所述判断所述目标设备是否为可信任设备的步骤，否则，拒绝所述设备连接请求。

[0019] 可选的，在其中一个实施例中，所述判断所述目标设备是否为可信任设备的步骤之后还包括：

[0020] 在所述目标设备不为可信任设备时，接收用户输入的设备添加指令；

[0021] 根据所述设备添加指令，将所述目标设备标识添加至所述预设的可信任设备列表。

[0022] 可选的，在其中一个实施例中，所述方法还包括：

[0023] 检测与目标设备对应数据传输流量，在所述数据传输流量大于预设的流量阈值的情况下，暂停与所述目标设备之间的数据传输，并生成提示消息进行展示；

[0024] 检测针对所述提示消息输入的操作指令，所述操作指令包括数据传输继续指令和设备连接断开指令；

[0025] 在所述操作指令为数据传输继续指令时，移除对与所述数据传输的暂停状态；

[0026] 在所述操作指令为设备连接断开指令时，断开与所述目标设备之间的通信连接。

[0027] 此外，本发明实施例还提出了一种设备连接的装置。

[0028] 一种设备连接的装置，包括：

[0029] 设备连接请求接收模块，用于接收设备连接请求，获取所述设备连接请求携带的目标设备标识，所述目标设备标识对应于目标设备；

[0030] 通信连接建立模块，用于判断所述目标设备是否为可信任设备，在所述目标设备为可信任设备时，建立与目标设备之间的通信连接；

[0031] 信任等级确定模块，用于获取与所述目标设备对应的信任等级，确定与所述目标设备对应的信任等级对应的可访问文件；

[0032] 数据访问请求检测模块，用于检测目标设备发送的数据访问请求，获取与所述数据访问请求对应的目标数据；

[0033] 数据访问请求响应模块，用于判断目标数据是否属于所述可访问文件，在所述目标数据属于所述可访问文件时，将所述目标数据的访问路径返回给所述目标设备，在所述目标数据不属于所述可访问文件时，拒绝所述文件访问请求。

[0034] 可选的，在其中一个实施例中，所述信任等级确定模块还用于获取与目标设备对应的历史连接记录，所述历史连接记录包括历史连接次数和/或历史连接时长；根据预设的信任等级计算公式，以所述历史连接次数和/或历史连接时长为自变量计算与所述目标设备对应的信任等级。

[0035] 可选的，在其中一个实施例中，所述通信连接建立模块还用于在预设的可信任设备列表中查找与所述目标设备标识匹配的设备标识，在查找到时，判定所述目标设备为可信任设备。

[0036] 可选的，在其中一个实施例中，所述装置还包括密码验证模块，用于接收所述目标设备发送的密码，所述密码由所述目标设备根据检测到的在目标设备上输入的字符串生成；判断所述密码是否与预设值匹配，若是，则执行所述判断所述目标设备是否为可信任设备的步骤，否则，拒绝所述设备连接请求。

[0037] 可选的，在其中一个实施例中，所述通信连接建立模块还用于在所述目标设备不为可信任设备时，接收用户输入的设备添加指令；根据所述设备添加指令，将所述目标设备标识添加至所述预设的可信任设备列表。

[0038] 可选的，在其中一个实施例中，所述装置还包括数据传输流量控制模块，用于检测与目标设备对应数据传输流量，在所述数据传输流量大于预设的流量阈值的情况下，暂停与所述目标设备之间的数据传输，并生成提示消息进行展示；检测针对所述提示消息输入的操作指令，所述操作指令包括数据传输继续指令和设备连接断开指令；在所述操作指令为数据传输继续指令时，移除对与所述数据传输的暂停状态；在所述操作指令为设备连接断开指令时，断开与所述目标设备之间的通信连接。

[0039] 采用了上述设备连接的方法和装置之后，在目标设备发起对本地设备的蓝牙连接、WiFi连接或其他连接请求时，需要首先对目标设备是否为可信任设备进行判断，只有在目标设备为可信任设备的情况下，才能将目标设备与本地设备连接起来并进行数据的访问或传输。并且，每一个可信任设备均存在一个与之对应的信任等级，信任等级决定了目标设备在本地设备上的访问权限以及其具体可访问的数据，只有在目标设备需要访问的数据属于上述信任等级对应的可访问的数据的情况下才能访问该数据，反之，则不能访问该数据。也就是说，通过对可信任设备的判断以及是否具备数据的访问权限来限制了目标设备对于本地设备上的数据的访问和传输，相较于传统技术中通过简单的PIN码即可访问所有的用户数据的方案，提高了设备之间建立连接和数据传输的安全性。

附图说明

[0040] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0041] 其中：

[0042] 图1为一个实施例中一种设备连接的方法的流程示意图；

[0043] 图2为一个实施例中一种设备连接的装置的结构示意图；

[0044] 图3为一个实施例中运行前述设备连接的方法的计算机设备的结构示意图。

具体实施方式

[0045] 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作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。

[0046] 在本实施例中，特提出了一种设备连接的方法，该方法的实现可依赖于计算机程

序，该计算机程序可运行于基于冯诺依曼体系的计算机系统之上，该计算机程序可以是设备或终端之间的连接管理应用程序，例如，蓝牙连接的管理程序或者WiFi连接的管理程序。该计算机系统可以是运行上述计算机程序的例如智能手机、平板电脑、个人电脑等服务器或终端。

[0047] 需要说明的是，在本实施例中，两个设备之间的连接可以是蓝牙连接，也可以是WiFi连接，还可以是其他通信连接方式，并且，在通信连接建立之后，两个互相连接的设备之间可以进行数据的交互。

[0048] 具体的，如图1所示，上述设备连接的方法包括如下步骤：

[0049] 步骤S102：接收设备连接请求，获取所述设备连接请求携带的目标设备标识，所述目标设备标识对应于目标设备。

[0050] 在本实施例中，执行主体为例如智能手机、平板电脑等终端设备，在该终端设备上还设置有相应的功能模块，例如，在两个设备之间的连接为蓝牙连接时，在本地的终端设备上设置有蓝牙模块，再例如，在两个设备之间的连接为WiFi连接时，在本地的终端设备上也设置有WiFi模块。需要说明的是，不仅在本地的终端设备上设置有相应的蓝牙模块或者WiFi模块，在与本地的终端设备连接的另一设备上也需要设置有对应的蓝牙模块或者WiFi模块。

[0051] 在本实施例中，目标设备可以向本地的终端设备(以下称本地设备)发起设备连接请求，例如，目标设备可以在蓝牙管理页面或者蓝牙连接页面，向可连接的蓝牙设备列表中的某一设备发起设备连接请求，在目标设备发起设备连接请求之后，该设备可以接收到目标设备发起的设备连接请求。

[0052] 在目标设备向本地设备发起设备连接请求时，本地设备会检测到目标设备发送的设备连接请求，并且，在接收到该设备连接请求之后，对接收到的设备连接请求进行解析，获取在设备连接请求中携带的相关信息。在本实施例中，在设备连接请求中携带有发起设备连接请求的目标设备对应的目标设备标识，并且，根据该目标设备标识可以确定相应的设备。

[0053] S104：判断所述目标设备是否为可信任设备，若是，则执行步骤S1060：建立与目标设备之间的通信连接，若否，则执行步骤S1062：拒绝所述设备连接请求。

[0054] 在目标设备发起了设备连接请求之后，本地设备可以选择与该目标设备建立通信连接或者拒绝响应该设备连接请求，上述具体的选择可以由用户手动选择，还可以是根据该目标设备是否为安全设备或者可信任设备来确定。

[0055] 例如，用户可以将经常会建立通信连接的设备标识为可信任设备，在被标识为可信任设备的设备向本地设备发起通信连接的情况下，直接默认可以建立本地设备与目标设备之间的通信连接。又例如，可以在终端中设置有可信任设备列表，在接收到的设备连接请求对应的目标设备属于该可信任设备列表时，默认可以直接建立该目标设备与本地设备之间的通信连接。

[0056] 具体的，上述判断所述目标设备是否为可信任设备的步骤还包括：在预设的可信任设备列表中查找与所述目标设备标识匹配的设备标识，若查找到，则判定所述目标设备为可信任设备。

[0057] 也就是说，在接收到设备连接请求之后，获取该设备连接请求的发起方对应的目

标设备标识，并且在终端中存储的预设的可信任设备列表中查找与该目标设备标识匹配的设备标识，若查找到，则说明目标设备标识对应的目标设备属于该可信任设备列表，即目标设备为可信任设备。反之，若没有查找到，则说明目标设备不属于该可信任设备列表，当前的设备连接可能存在安全隐患。

[0058] 需要说明的是，在本实施例中，判断一个设备是否为可信任设备的方式不限于上述给出的判断方式，还可以是其他任意的可行的判断方式，例如，可以根据本地设备与目标设备之间的历史连接记录来确定，也就是说，根据本地设备与目标设备之间的历史连接的频率、时长、数据访问记录和数据传输记录等相关历史连接记录。

[0059] 进一步的，若目标设备与本地设备之间没有历史的连接记录，则说明二者之间在此之前没有相关性，因此，该目标设备不可能被判定为可信任设备。为了避免这种情况下一律的被判定为不可信任设备或无法建立本地设备或目标设备之间的通信连接，并增加设备之间是否连接的可操作性，在一个实施例中，上述判断所述目标设备是否为可信任设备的步骤之后还包括：在所述目标设备不为可信任设备时，接收用户输入的设备添加指令；根据所述设备添加指令，将所述目标设备标识添加至所述预设的可信任设备列表。

[0060] 在本实施例中，若目标设备不是可信任设备，则无法建立目标设备与本地设备之间的通信连接，但是，在目标设备不是可信任设备的情况下，可以生成相应的提示信息并在本地设备上进行展示，以告知用户发起设备连接请求的目标设备不是可信任设备，因此无法建立与目标设备之间的通信连接。

[0061] 进一步的，在展示上述提示信息的同时，用户还可以针对上述展示的提示信息，输入相关的操作，例如，忽略该提示消息，或者，建立与目标设备之间的通信连接，再或者，将目标设备标识为可信任设备的操作指令。在上述判断目标设备是否为可信任设备时是通过预设的可信任设备列表来判断的情况下，若目标设备不是可信任设备，用户还可以输入设备添加指令，将目标设备添加到上述可信任设备列表中去，也就是说，在目标设备再次发起设备连接请求时，会因为目标设备已经添加到了可信任设备列表，从而建立本地设备与目标设备之间的通信连接。

[0062] 需要说明的是，在本实施例中，将目标设备添加到可信任设备列表的过程可以是将目标设备标识添加到可信任设备列表中去的过程。

[0063] 可选的，在一个实施例中，为了进一步的提高两个设备之间建立设备连接的过程中的安全性，进一步的保证用户数据的安全性，两个设备之间建立通信连接不仅需要对应的设备是可信任设备，还需要进行身份验证。

[0064] 具体的，在一个实施例中，上述接收设备连接请求的步骤之后还包括：接收所述目标设备发送的密码，所述密码由所述目标设备根据检测到的在目标设备上输入的字符串生成；判断所述密码是否与预设值匹配，若是，则执行所述判断所述目标设备是否为可信任设备的步骤，否则，拒绝所述设备连接请求。

[0065] 也就是说，在本地设备接收到了目标设备发送的设备连接请求之后，响应该设备连接请求，并返回相应的身份验证请求给目标设备。目标设备在接收到了本地设备返回的身份验证请求之后，提示用户在目标设备上输入密码，并将检测到的密码返回给本地设备，由本地设备判断目标设备返回的密码是否通过。

[0066] 例如，在一个实施例中，在上述设备连接为蓝牙连接的情况下，上述密码即为PIN

码，也就是说，本地设备设置一个PIN码，若用户在目标设备上输入的PIN码与本地设备设置的PIN码匹配的情况下，即判定身份验证通过。

[0067] 需要说明的是，在本实施例中，上述利用密码进行身份验证的过程不仅仅可以是在判断目标设备是否为可信任设备之前，还可以是在判定了目标设备为可信任设备之后，在建立通信连接之前。

[0068] 步骤S108：获取与所述目标设备对应的信任等级，确定与所述目标设备对应的信任等级对应的可访问文件。

[0069] 在本实施例中，目标设备与本地终端建立了通信连接之后，并不能一律访问本地设备上的所有数据，例如，可以设置不同的访问权限，某一访问权限下目标设备可以访问本地设备上的所有图片格式的文件，另一访问权限下目标设备可以访问本地设备上的SD卡的所有数据但是不能访问本地设备上非SD卡上的所有数据，等等，可以根据需要设置不同的访问权限。

[0070] 在本地终端中，用户可以设置与每一个可信任设备对应的信任等级，每一个信任等级都对应了相应的访问权限，访问权限决定了目标设备可以在本地设备上访问的文件，即可访问文件，也就是说，信任等级决定了目标设备可访问的可访问文件。

[0071] 在另一个实施例中，还可以是根据目标设备与本地设备之间的历史连接记录确定与目标设备对应的信任等级，例如，在历史连接的次数多、频率高、连接的时长大的情况下，其对应的信任等级就越高，并且，对应的可访问的文件越多。

[0072] 具体的，所述获取与所述目标设备对应的信任等级的步骤还包括：获取与目标设备对应的历史连接记录，所述历史连接记录包括历史连接次数和/或历史连接时长；根据预设的信任等级计算公式，以所述历史连接次数和/或历史连接时长为自变量计算与所述目标设备对应的信任等级。

[0073] 也就是说，可以根据预设的信任等级计算公式，计算与目标设备对应的历史连接记录对应的信任等级。例如，每增加一次历史连接次数，计1分，连接时长每增加1h，计1分，等，并且将所有的计分的总和即为最终的信用分数，并且，针对信用分数进行区间划分，每一个区间对应一个信任等级。

[0074] 步骤S110：检测目标设备发送的数据访问请求，获取与所述数据访问请求对应的目标数据。

[0075] 在目标设备与本地设备之间的通信连接建立成功之后，二者之间即可互相访问另一方设备上的数据，并且将对方的数据拷贝到本设备上。例如，目标设备可以通过发起数据访问请求访问本地设备上的某一个目标数据。

[0076] 目标数据可以是文件或文件夹，例如，相册、日志、联系人资料、系统文件等。目标数据标识即为用于访问目标数据的文件名或文件路径。例如，若目标设备要访问本地设备的相册中的某张照片，则需要输入该照片的文件路径，并根据该输入的文件路径生成数据访问请求；或者访问该照片所在的目录，相册应用遍历该目录下的照片的文件路径，获取缩略图展示给用户。手机操作系统在遍历该目录下的照片的文件路径时，即生成了数据访问请求。

[0077] 也就是说，用户在目标设备上输入的数据访问请求中必定对应了当前需要访问的具体的目标数据。但是，根据上述访问权限以及信任等级的设置，并不是本地设备上的所有

数据都可以被目标设备所访问，因此，还需要确定目标设备是否具有访问该目标数据的访问权限。

[0078] 步骤S112：判断目标数据是否属于所述可访问文件，若是，则执行步骤S1140：将所述目标数据的访问路径返回给所述目标设备，若否，则执行步骤S1142：拒绝所述文件访问请求。

[0079] 也就是说，需要确定当前需要访问的目标数据是否属于上述根据目标设备的信任等级确定的可访问文件，若不是，则访问目标数据失败，在一个实施例中，可生成相应的数据访问失败的提示消息并在目标设备和/或本地设备上进行展示。进一步的，若当前需要访问的目标数据属于上述可访问文件，则说明目标设备具有访问目标数据的访问权限，则继续访问目标数据。具体的，将目标数据的访问路径返回给目标设备，目标设备可以通过上述访问路径读取目标数据。

[0080] 进一步的，目标设备还可以将目标数据拷贝到目标设备本地，即本地设备将与目标数据对应的数据经过本地设备与目标设备之间的通信连接传输给目标设备，由目标设备存储在目标设备本地的存储区域中。

[0081] 可选的，在一个实施例中，为了保证在建立了设备连接建立成功的情况下的用户数据的安全性，避免其他用户从本地设备上拷贝了过多的数据，还需要对在设备连接的情况下的数据传输的数据量进行控制。

[0082] 具体的，本方法还包括：检测与目标设备对应数据传输流量，在所述数据传输流量大于预设的流量阈值的情况下，暂停与所述目标设备之间的数据传输，并生成提示消息进行展示；检测针对所述提示消息输入的操作指令，所述操作指令包括数据传输继续指令和设备连接断开指令；在所述操作指令为数据传输继续指令时，移除对与所述数据传输的暂停状态；在所述操作指令为设备连接断开指令时，断开与所述目标设备之间的通信连接。

[0083] 也就是说，在设备连接建立成功之后，建立一个监控相应的数据流量进程，用来检测目标设备访问本地设备上的数据的数据流量，该数据流量可以是数据访问流量，也可以是数据传输流量。

[0084] 在本实施例中，设置有流量阈值，该流量阈值用来显示上述数据流量的最大值，也就是说，目标设备与本地设备之间的数据访问或数据传输的最大数据量不能超过上述流量阈值，若超过了该流量阈值，就需要暂停目标设备与本地设备之间的数据传输或数据访问，并且生成相应的提示消息并展示给用户，以提示当前的数据传输或数据访问的数据量已达到最大值，数据传输和数据访问被暂停。

[0085] 进一步的，在上述数据流量超过预设的流量阈值的情况下，若用户需要继续访问本地设备上的相关数据，可以在本地设备上输入继续访问或继续传输的操作指令，也就是说，用户可以通过本地设备输入数据传输继续指令，以使所述数据传输的暂停状态被移除被继续之前被暂停的数据传输；在另一个实施例中，用户还可以通过本地设备输入设备连接断开指令，断开目标设备与本地设备之间的通信连接，从而终止目标设备与本地设备之间的数据传输。

[0086] 进一步的，在一个实施例中，目标设备与本地设备之间的通信连接的连接时间是有限制的，避免其他用户利用二者之间的通信连接切换设备上的用户数据，也就是说，针对目标设备与本地设备之间的设备连接时间设置一个定时器，在定时器被唤醒的情况下，断

开目标设备与本地设备之间的通信连接。

[0087] 此外，在一个实施例中，如图2所示，还提出了一种设备连接的装置，包括设备连接请求接收模块102、通信连接建立模块104、信任等级确定模块106、数据访问请求检测模块108以及数据访问请求响应模块110，其中：

[0088] 设备连接请求接收模块102，用于接收设备连接请求，获取所述设备连接请求携带的目标设备标识，所述目标设备标识对应于目标设备；

[0089] 通信连接建立模块104，用于判断所述目标设备是否为可信任设备，在所述目标设备为可信任设备时，建立与目标设备之间的通信连接；

[0090] 信任等级确定模块106，用于获取与所述目标设备对应的信任等级，确定与所述目标设备对应的信任等级对应的可访问文件；

[0091] 数据访问请求检测模块108，用于检测目标设备发送的数据访问请求，获取与所述数据访问请求对应的目标数据；

[0092] 数据访问请求响应模块110，用于判断目标数据是否属于所述可访问文件，在所述目标数据属于所述可访问文件时，将所述目标数据的访问路径返回给所述目标设备，在所述目标数据不属于所述可访问文件时，拒绝所述文件访问请求。

[0093] 可选的，在一个实施例中，所述信任等级确定模块106还用于获取与目标设备对应的历史连接记录，所述历史连接记录包括历史连接次数和/或历史连接时长；根据预设的信任等级计算公式，以所述历史连接次数和/或历史连接时长为自变量计算与所述目标设备对应的信任等级。

[0094] 可选的，在一个实施例中，所述通信连接建立模块104还用于在预设的可信任设备列表中查找与所述目标设备标识匹配的设备标识，在查找到时，判定所述目标设备为可信任设备。

[0095] 可选的，在一个实施例中，如图2所示，上述装置还包括密码验证模块112，用于接收所述目标设备发送的密码，所述密码由所述目标设备根据检测到的在目标设备上输入的字符串生成；判断所述密码是否与预设值匹配，若是，则执行所述判断所述目标设备是否为可信任设备的步骤，否则，拒绝所述设备连接请求。

[0096] 可选的，在一个实施例中，所述通信连接建立模块104还用于在所述目标设备不为可信任设备时，接收用户输入的设备添加指令；根据所述设备添加指令，将所述目标设备标识添加至所述预设的可信任设备列表。

[0097] 可选的，在一个实施例中，如图2所示，上述装置还包括数据传输流量控制模块114，用于检测与目标设备对应数据传输流量，在所述数据传输流量大于预设的流量阈值的情况下，暂停与所述目标设备之间的数据传输，并生成提示消息进行展示；检测针对所述提示消息输入的操作指令，所述操作指令包括数据传输继续指令和设备连接断开指令；在所述操作指令为数据传输继续指令时，移除对与所述数据传输的暂停状态；在所述操作指令为设备连接断开指令时，断开与所述目标设备之间的通信连接。

[0098] 采用了上述设备连接的方法和装置之后，在目标设备发起对本地设备的蓝牙连接、WiFi连接或其他连接请求时，需要首先对目标设备是否为可信任设备进行判断，只有在目标设备为可信任设备的情况下，才能将目标设备与本地设备连接起来并进行数据的访问或传输。并且，每一个可信任设备均存在一个与之对应的信任等级，信任等级决定了目标设

备在本地设备上的访问权限以及其具体可访问的数据，只有在目标设备需要访问的数据属于上述信任等级对应的可访问的数据的情况下才能访问该数据，反之，则不能访问该数据。也就是说，通过对可信任设备的判断以及是否具备数据的访问权限来限制了目标设备对于本地设备上的数据的访问和传输，相较于传统技术中通过简单的PIN码即可访问所有的用户数据的方案，提高了设备之间建立连接和数据传输的安全性。

[0099] 在一个实施例中，如图3所示，图3展示了一种运行上述设备连接的方法的基于冯诺依曼体系的计算机系统的终端。该计算机系统可以是智能手机、平板电脑、掌上电脑、笔记本电脑或个人电脑等终端设备。具体的，可包括通过系统总线连接的外部输入接口1001、处理器1002、存储器1003和输出接口1004。其中，外部输入接口1001可选的可至少包括网络接口10012。存储器1003可包括外存储器10032(例如硬盘、光盘或软盘等)和内存储器10034。输出接口1004可至少包括显示屏10042等设备。

[0100] 在本实施例中，本方法的运行基于计算机程序，该计算机程序的程序文件存储于前述基于冯诺依曼体系的计算机系统的外存储器10032中，在运行时被加载到内存储器10034中，然后被编译为机器码之后传递至处理器1002中执行，从而使得基于冯诺依曼体系的计算机系统中形成逻辑上的设备连接请求接收模块102、通信连接建立模块104、信任等级确定模块106、数据访问请求检测模块108、数据访问请求响应模块110、密码验证模块112以及数据传输流量控制模块114。且在上述设备连接的.方法执行过程中，输入的参数均通过外部输入接口1001接收，并传递至存储器1003中缓存，然后输入到处理器1002中进行处理，处理的结果数据或缓存于存储器1003中进行后续地处理，或被传递至输出接口1004进行输出。

[0101] 具体的，上述处理器1002用于执行如下操作：

[0102] 接收设备连接请求，获取所述设备连接请求携带的目标设备标识，所述目标设备标识对应于目标设备；

[0103] 判断所述目标设备是否为可信任设备，若为可信任设备，则建立与目标设备之间的通信连接；

[0104] 获取与所述目标设备对应的信任等级，确定与所述目标设备对应的信任等级对应的可访问文件；

[0105] 检测目标设备发送的数据访问请求，获取与所述数据访问请求对应的目标数据；

[0106] 判断目标数据是否属于所述可访问文件，若所述目标数据属于所述可访问文件，则将所述目标数据的访问路径返回给所述目标设备，否则，拒绝所述文件访问请求。

[0107] 在一个可选的实施例中，上述处理器1002还用于执行获取与目标设备对应的历史连接记录，所述历史连接记录包括历史连接次数和/或历史连接时长；根据预设的信任等级计算公式，以所述历史连接次数和/或历史连接时长为自变量计算与所述目标设备对应的信任等级。

[0108] 在一个可选的实施例中，上述处理器1002还用于执行在预设的可信任设备列表中查找与所述目标设备标识匹配的设备标识，若查找到，则判定所述目标设备为可信任设备。

[0109] 在一个可选的实施例中，上述处理器1002还用于执行接收所述目标设备发送的密码，所述密码由所述目标设备根据检测到的在目标设备上输入的字符串生成；判断所述密码是否与预设值匹配，若是，则执行所述判断所述目标设备是否为可信任设备的步骤，否

则，拒绝所述设备连接请求。

[0110] 在一个可选的实施例中，上述处理器1002还用于执行在所述目标设备不为可信任设备时，接收用户输入的设备添加指令；根据所述设备添加指令，将所述目标设备标识添加至所述预设的可信任设备列表。

[0111] 在一个可选的实施例中，上述处理器1002还用于执行：检测与目标设备对应数据传输流量，在所述数据传输流量大于预设的流量阈值的情况下，暂停与所述目标设备之间的数据传输，并生成提示消息进行展示；检测针对所述提示消息输入的操作指令，所述操作指令包括数据传输继续指令和设备连接断开指令；在所述操作指令为数据传输继续指令时，移除对与所述数据传输的暂停状态；在所述操作指令为设备连接断开指令时，断开与所述目标设备之间的通信连接。

[0112] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

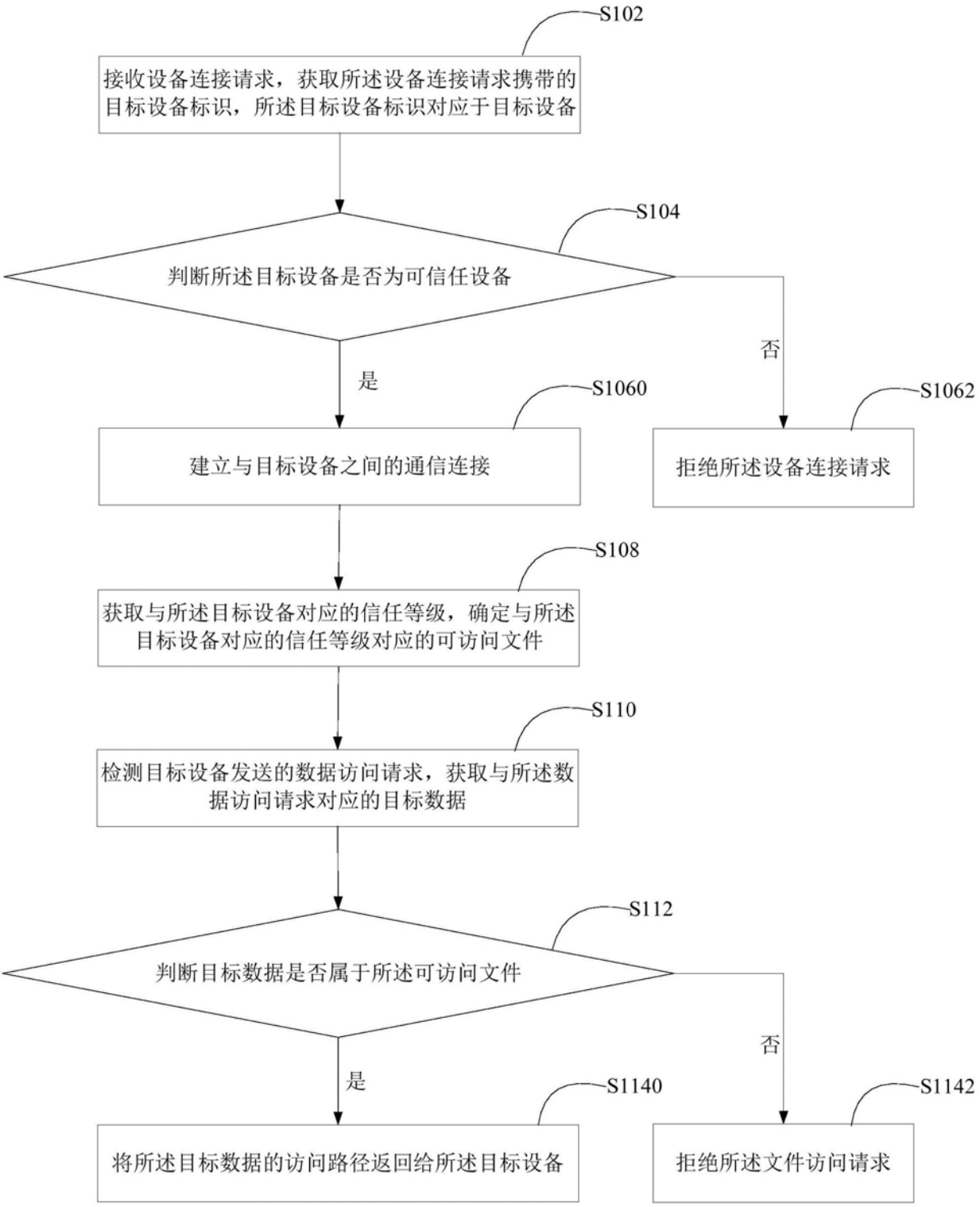

S102
接收设备连接请求，获取所述设备连接请求携带的目标设备标识，所述目标设备标识对应于目标设备
S104
判断所述目标设备是否为可信任设备
否
是
S1060
建立与目标设备之间的通信连接
S1062
拒绝所述设备连接请求
S108
获取与所述目标设备对应的信任等级，确定与所述目标设备对应的信任等级对应的可访问文件
S110
检测目标设备发送的数据访问请求，获取与所述数据访问请求对应的目标数据
S112
判断目标数据是否属于所述可访问文件
否
是
S1140
将所述目标数据的访问路径返回给所述目标设备
S1142
拒绝所述文件访问请求

图1

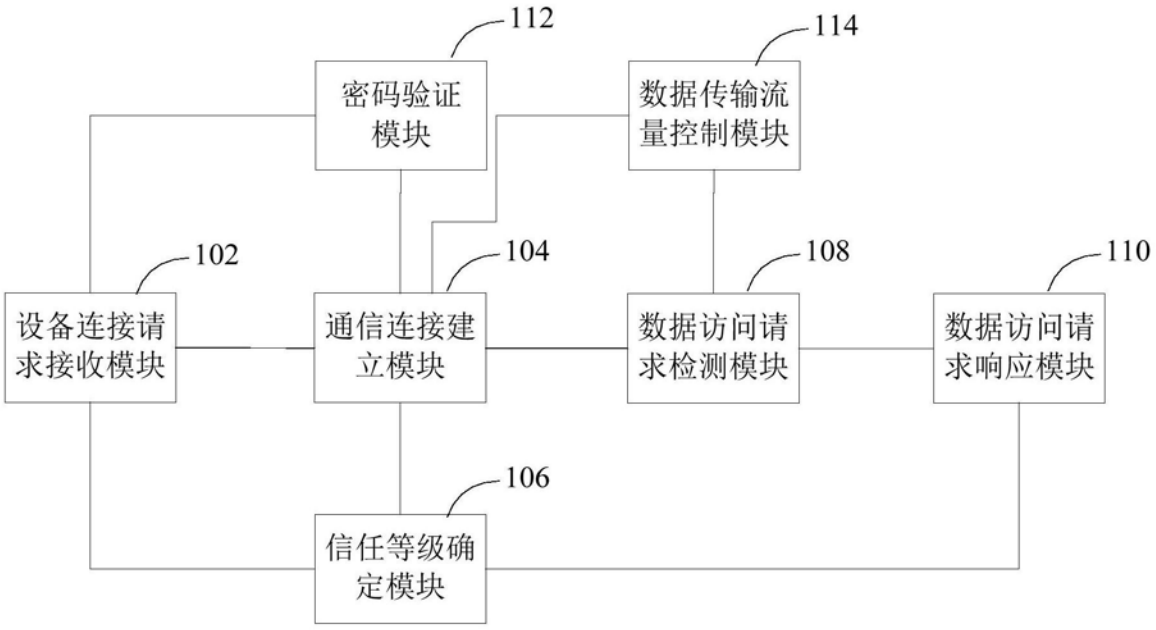

112
密码验证模块
114
数据传输流量控制模块
102
设备连接请求接收模块
104
通信连接建立模块
108
数据访问请求检测模块
110
数据访问请求响应模块
106
信任等级确定模块

图2

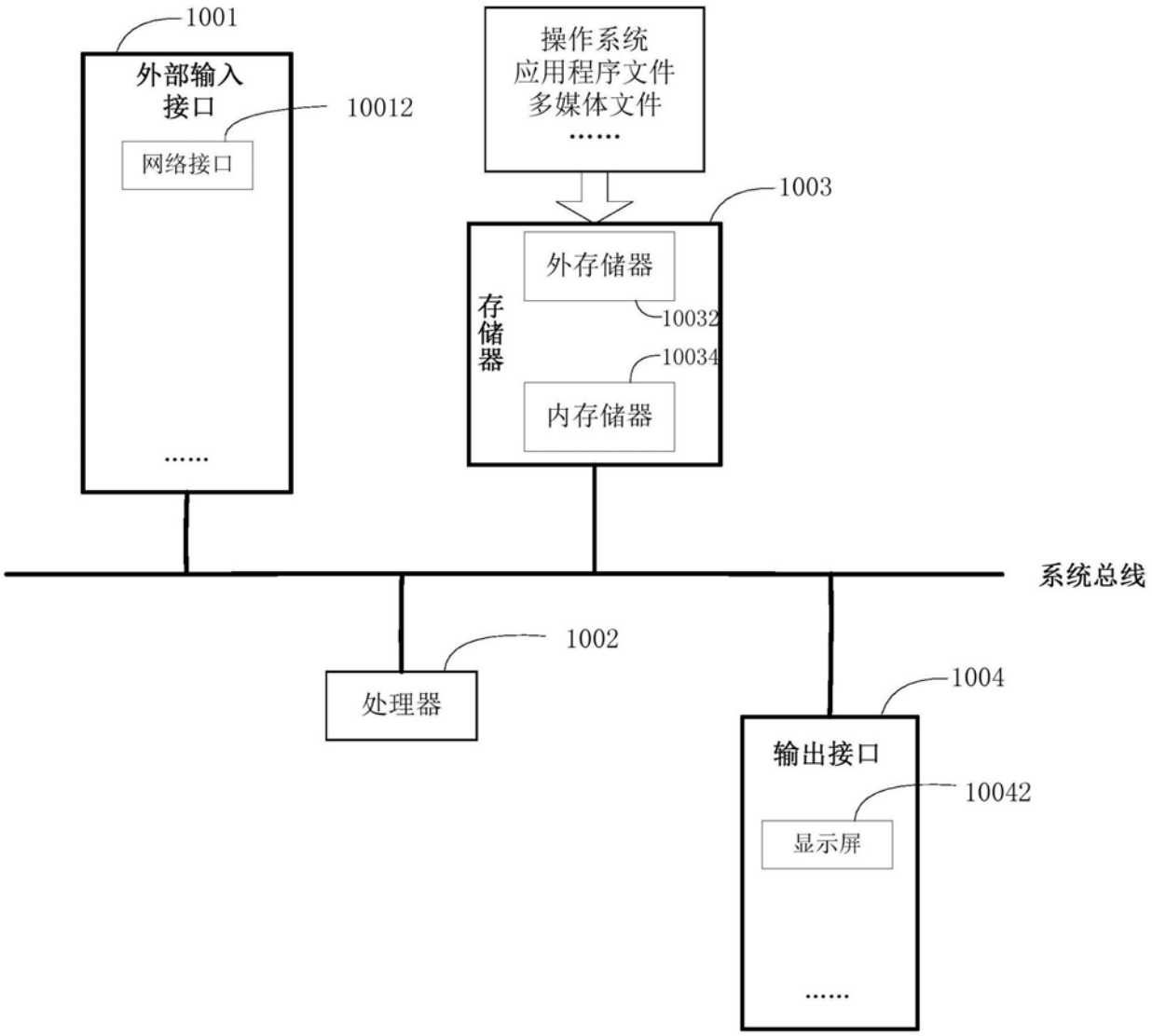

1001
外部输入
接口
10012
网络接口
.....
操作系统
应用程序文件
多媒体文件
.....
1003
外存储器
10032
存
储
器
10034
内存储器
系统总线
1002
处理器
1004
输出接口
10042
显示屏
.....

图3