

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 5 月 3 日 (03.05.2018)



(10) 国际公布号
WO 2018/076863 A1

- (51) 国际专利分类号:
G06F 21/56 (2013.01)
- (21) 国际申请号: PCT/CN2017/095618
- (22) 国际申请日: 2017 年 8 月 2 日 (02.08.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610949089.5 2016 年 10 月 25 日 (25.10.2016) CN
- (71) 申请人: 广东欧珀移动通信有限公司 (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.) [CN/CN]; 中国广
- 东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。
- (72) 发明人: 马志峰 (MA, Zhifeng); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。
- (74) 代理人: 深圳翼盛智成知识产权事务所(普通合伙) (ESSEN PATENT&TRADEMARK AGENCY); 中国广东省深圳市福田区深南大道 6021 号喜年中心 A 座 1709-1711, Guangdong 518040 (CN)。
- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

(54) Title: DATA STORAGE METHOD, APPARATUS, STORAGE MEDIUM, SERVER AND SYSTEM

(54) 发明名称: 数据存储的方法、装置、存储介质、服务器及系统

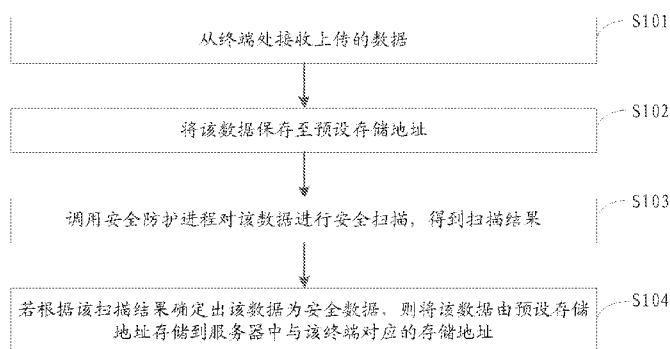


图 1

S101 RECEIVING UPLOADED DATA FROM A TERMINAL
S102 SAVING THE DATA TO A PRESET STORAGE ADDRESS
S103 CALLING A SECURITY PROCESS TO SCAN THE DATA SECURELY SO AS TO OBTAIN A SCAN RESULT
S104 STORING THE DATA FROM THE PRESET STORAGE ADDRESS TO A STORAGE ADDRESS IN A SERVER WHICH CORRESPONDS TO THE TERMINAL IF DETERMINED FROM THE SCAN RESULT THAT THE DATA IS SECURE DATA

(57) Abstract: A data storage method, comprising: receiving uploaded data from a terminal (S101); saving the data to a preset storage address (S102); calling a security process to scan the data securely so as to obtain a scan result (S103); and storing the data from the preset storage address to a storage address in a server which corresponds to the terminal if determined from the scan result that the data is secure data (S104). Said method may improve the security of data stored in a server.

(57) 摘要: 一种数据存储的方法, 包括: 从终端处接收上传的数据 (S101); 将该数据保存至预设存储地址 (S102); 调用安全防护进程对该数据进行安全扫描, 得到扫描结果 (S103); 若根据该扫描结果确定出该数据为安全数据, 则将该数据由预设存储地址存储到服务器中与该终端对应的存储地址 (S104)。所述方法可以提高服务器存储的数据的安全性。

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

数据存储的方法、装置、存储介质、服务器及系统

- [1] 本申请要求于2016年10月25日提交中国专利局、申请号为201610949089.5、发明名称为“数据存储的方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

- [2] 本发明属于通信技术领域，尤其涉及一种数据存储的方法、装置、存储介质、服务器及系统。

背景技术

- [3] 随着信息数据交流越来越频繁，使用云存储服务的用户也越来越多。借助于云存储服务，终端可以将用户使用过程中产生的数据上传到对应的云存储服务器中予以备份，并在有需要的时候从云存储服务器中将数据下载到终端。

对发明的公开

技术问题

- [4] 本发明实施例提供一种数据存储的方法、装置、存储介质、服务器及系统，能提高服务器存储的数据的安全性。

问题的解决方案

技术解决方案

- [5] 本发明实施例提供一种数据存储的方法，包括：
- [6] 从终端处接收上传的数据；
- [7] 将所述数据保存至预设存储地址；
- [8] 调用安全防护进程对所述数据进行安全扫描，得到扫描结果；
- [9] 若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [10] 本发明实施例还提供一种数据存储的装置，包括：
- [11] 接收单元，用于从终端处接收上传的数据；
- [12] 保存单元，用于将所述数据保存至预设存储地址；

- [13] 扫描单元，用于调用安全防护进程对所述数据进行安全扫描，得到扫描结果；
- [14] 存储单元，用于若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [15] 本发明实施例提供一种存储介质，其上存储有计算机程序，当所述计算机程序在计算机上执行时，使得所述计算机执行如本发明实施例提供的数据存储的方法。
- [16] 本发明实施例提供一种服务器，包括存储器，处理器，所述处理器通过调用所述存储器中存储的计算机程序，用于执行如下步骤：
- [17] 从终端处接收上传的数据；
- [18] 将所述数据保存至预设存储地址；
- [19] 调用安全防护进程对所述数据进行安全扫描，得到扫描结果；
- [20] 若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [21] 本发明实施例还提供一种数据存储的系统，包括服务器和终端，所述服务器包括上述的数据存储的装置。

发明的有益效果

有益效果

- [22] 本发明实施例提供一种数据存储的方法、装置、存储介质、服务器及系统，能提高服务器存储的数据的安全性。

对附图的简要说明

附图说明

- [23] 下面结合附图，通过对本发明的具体实施方式详细描述，将使本发明的技术方案及其有益效果显而易见。
- [24] 图1是本发明实施例提供的数据存储的方法的流程示意图。
- [25] 图2是本发明实施例提供的数据存储的方法的另一流程示意图。
- [26] 图3是本发明实施例提供的数据存储的装置的结构示意图。
- [27] 图4是本发明实施例提供的数据存储的装置的另一结构示意图。
- [28] 图5是本发明实施例提供的数据存储的系统的场景示意图。

[29] 图6是本发明实施例提供的服务器的结构示意图。

[30] 图7是本发明实施例提供的服务器的另一结构示意图。

实施该发明的最佳实施例

本发明的最佳实施方式

[31] 请参照图式，其中相同的组件符号代表相同的组件，本发明的原理是以实施在一适当的运算环境中来举例说明。以下的说明是基于所例示的本发明具体实施例，其不应被视为限制本发明未在此详述的其它具体实施例。

[32] 在实际使用过程中，如果用户终端在使用过程中已经感染了如木马等计算机病毒，那么终端上传到云存储服务器中的数据也很可能携带有计算机病毒，这将对云存储服务器中的数据安全构成威胁。

[33] 本发明实施例提供一种数据存储的方法，包括：

[34] 从终端处接收上传的数据；

[35] 将所述数据保存至预设存储地址；

[36] 调用安全防护进程对所述数据进行安全扫描，得到扫描结果；

[37] 若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。

[38] 在一种实施方式中，在所述得到扫描结果的步骤之后，还可以包括：若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除。

[39] 在一种实施方式中，所述若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除的步骤，可以包括：若根据所述扫描结果确定出所述数据为不安全数据，则调用安全处理进程对所述数据进行处理；若检测到所述数据经过处理后未变为安全数据，则将所述数据从预设存储地址中删除。

[40] 在一种实施方式中，在所述调用安全处理进程对所述数据进行处理步骤之后，还可以包括：若检测到所述数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与所述终端对应的存储地址。

[41] 在一种实施方式中，在所述将所述数据从预设存储地址中删除的步骤之后，还

可以包括：发送提示信息至所述终端，所述提示信息用于提示所述终端上传的数据为不安全数据，并被服务器删除。

[42] 在一种实施方式中，在所述将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址的步骤之后，还可以包括：清空所述预设存储地址中的数据。

[43] 在一种实施方式中，在所述将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址的步骤之后，还可以包括：向所述终端发送用于提示所述终端上传的数据为安全数据，并被存储到与所述终端对应的存储地址的信息。

[44] 请参阅图1，图1是本发明实施例提供的数据存储的方法的流程示意图，流程可以包括：

[45] 在步骤S101中，从终端处接收上传的数据。

[46] 在步骤S102中，将该数据保存至预设存储地址。

[47] 在本发明实施例的步骤S101和S102中，当服务器接收到终端上传的数据时，服务器先将该数据存储到一个指定的存储空间，即预设存储地址中。

[48] 需要说明的是，预设存储地址是一个用于临时存储终端所上传的数据的存储空间，有别于服务器中与各个终端对应的存储空间。例如，在服务器中，甲终端对应的存储地址为第一存储地址，乙终端对应的存储地址为第二存储地址，等等。而预设存储地址是不同于第一存储地址以及第二存储地址的一个存储空间。例如当接收到甲终端上传的数据时，服务器先将该数据保存在预先指定的预设存储地址，而不是立即保存到第一存储地址。之后，若接收到乙终端上传的数据，那么服务器也是先将乙终端上传的数据保存到预设存储地址中，而不是第二存储地址。

[49] 在步骤S103中，调用安全防护进程对该数据进行安全扫描，得到扫描结果。

[50] 比如，在服务器将终端上传的数据保存到预设存储地址之后，可以触发服务器调用安全防护进程对终端上传的数据进行安全扫描，并得到扫描结果。例如，服务器可以调用预设的杀毒软件（安全防护软件）对保存在预设存储地址中的数据进行安全扫描。在扫描结束后，该杀毒软件会向服务器上报一个扫描结果。

- [51] 在步骤S104中，若根据该扫描结果确定出该数据为安全数据，则将该数据由预设存储地址存储到服务器中与该终端对应的存储地址。
- [52] 比如，在得到扫描结果之后，如果服务器根据该扫描结果判断出终端上传的数据为安全数据，那么服务器就可以将该数据从预设存储地址存储到服务器中与该终端对应的存储地址中。例如，服务器在确定甲终端上传的数据为安全数据后，可以将该数据由预设存储地址剪切到服务器中与甲终端对应的第一存储地址保存起来。
- [53] 需要说明的是，当安全防护进程在终端上传的数据中未检测到计算机病毒、木马以及恶意程序等时，服务器会将终端上传的数据确定为安全数据。而如果安全防护进程在终端上传的数据中检测到了计算机病毒、木马以及恶意程序等，那么服务器会将终端上传的数据确定为不安全数据，等等。
- [54] 可以理解的是，在本发明实施例中，当接收到终端上传的数据时，服务器并不是立即将该数据保存到服务器中与该终端对应的存储空间中，而是先将该数据保存在某个指定的临时存储空间，并对该数据进行安全扫描。只有当在该数据中没有扫描到计算机病毒、木马或恶意程序等时，才会将该数据由临时存储空间存储到服务器中与该终端对应的存储空间。通过这种方式，可以有效避免服务器因接收到包含计算机病毒、木马或恶意程序的数据，而对存储在服务器中的大量数据造成安全威胁。
- [55] 请参阅图2，图2为本发明实施例提供的数据存储的方法的另一流程示意图，流程可以包括：
- [56] 在步骤S201中，服务器从终端处接收上传的数据。
- [57] 在步骤S202中，服务器将该数据保存至预设存储地址。
- [58] 比如，步骤S201和S202可以包括：
- [59] 当接收到终端上传的数据时，服务器可以先将该数据保存到指定的预设存储地址中。
- [60] 需要说明的是，预设存储地址是一个用于临时存储终端所上传的数据的存储空间，有别于服务器中与各个终端对应的存储空间。例如，在服务器中，甲终端对应的存储地址为第一存储地址，乙终端对应的存储地址为第二存储地址，等

等。而预设存储地址是不同于第一存储地址以及第二存储地址等的一个存储空间。

[61] 例如，当接收到甲终端上传的数据时，服务器可以先将该数据保存在预设存储地址中，而暂不保存到第一存储地址。

[62] 另外，由于预设存储地址为用于临时保存终端上传的数据的存储空间，因此，在服务器将临时保存在预设存储地址中的数据存储到与该终端对应的存储地址之后，服务器可以将该预设存储地址中的数据清空，以便该预设存储地址可以用于保存下一个终端上传的数据，等等。也即，在一种实施方式中，在服务器将终端上传的数据由预设存储地址存储到服务器中与该终端对应的存储地址之后，还可以包括如下步骤：清空该预设存储地址中的数据。

[63] 在步骤S203中，服务器调用安全防护进程对该数据进行安全扫描，得到扫描结果。

[64] 在步骤S204中，根据该扫描结果，服务器判断该数据是否为安全数据。

[65] 比如，在将终端上传的数据保存至预设存储地址之后，可以由服务器调用安全防护进程对该数据进行安全扫描，并得到扫描结果。例如，服务器可以调用预设的杀毒软件对终端上传的数据进行扫描。在扫描结束后，服务器可以获取到杀毒软件上报的扫描结果。

[66] 在获取到扫描结果后，服务器可以根据该扫描结果，判断终端上传的数据是否为安全数据。

[67] 需要说明的是，当扫描结果显示安全防护进程在终端上传的数据中未检测到计算机病毒、木马以及恶意程序等时，服务器可以将终端上传的数据确定为安全数据。而如果扫描结果显示安全防护进程在终端上传的数据中检测到了计算机病毒、木马以及恶意程序等，那么服务器可以将终端上传的数据确定为不安全数据，等等。

[68] 在步骤S205中，若判断出该数据为安全数据，则服务器将该数据由预设存储地址存储到服务器中与该终端对应的存储地址。

[69] 比如，在步骤S204中服务器判断出终端上传的数据为安全数据，那么可以触发服务器将终端上传的数据由预设存储地址存储到服务器中与该终端对应的存储

地址中。

[70] 例如，服务器确定出甲终端上传的数据为安全数据，那么服务器可以将甲终端上传的数据由预设存储地址剪切到服务器中与甲终端对应的第一存储地址。

[71] 在一种实施方式中，在上述服务器将终端上传的数据由预设存储地址存储到服务器中与该终端对应的存储地址的步骤之后，服务器还可以向该终端发送一则信息，该信息用于提示该终端上传的数据为安全数据，已存储到与该终端对应的存储地址中。在一种实施方式中，在服务器将终端上传的数据由预设存储地址存储到服务器中与该终端对应的存储地址的步骤之后，还可以包括如下步骤：向该终端发送用于提示该终端上传的数据为安全数据，并被存储到与该终端对应的存储地址的信息。

[72] 在步骤S206中，若判断出该数据为不安全数据，则服务器将该数据从预设存储地址中删除。

[73] 在步骤S207中，服务器发送提示信息至该终端，该提示信息用于提示该终端上传的数据为不安全数据，并被服务器删除。

[74] 比如，在步骤S204中服务器判断出终端上传的数据为不安全数据。那么，由于该终端本次上传的数据中包含有计算机病毒、木马或恶意程序等。因此，在这种情况下，服务器可以将该终端本次上传的数据从预设存储地址中删除。

[75] 之后，服务器还可以向该终端发送一则提示信息，该提示信息用于提示该终端其本次上传的数据因包含有计算机病毒、木马或恶意程序等，而被服务器删除。此外，该提示信息还可以提示终端启动安全防护软件对终端数据进行安全扫描，以查杀终端中隐藏的计算机病毒、木马或恶意程度等。或者，该提示信息还可以提示终端在查杀完毕隐藏在其中的计算机病毒、木马或恶意程序后，重新向服务器发送进行数据上传操作的请求，等等，此处不做具体限定。

[76] 在一种实施方式中，步骤S206中所述若根据该扫描结果确定出该数据为不安全数据，则服务器将该数据从预设存储地址中删除，可以包括：

[77] 若根据该扫描结果确定出该数据为不安全数据，则调用安全处理进程对该数据进行处理。

[78] 若检测到该数据经过处理后未变为安全数据，则将该数据从预设存储地址中删

除。

- [79] 比如，服务器根据安全防护进程的扫描结果判断出终端上传的数据为不安全数据，那么此时服务器还可以调用安全处理进程对终端上传的数据进行处理。例如，安全防护进程检测到终端上传的数据中包含有木马程序。此时，服务器可以调用预设的杀毒软件，对该数据进行木马程序清除处理。
- [80] 然而，由于杀毒软件的病毒库带有一定的局限性，杀毒软件无法对所有的计算机病毒、木马或恶意程序进行查杀。所以，若检测到终端上传的数据经过安全处理进程的处理后仍然为不安全的数据，也即安全处理进程无法消除终端上传的数据中携带的计算机病毒、木马或恶意程序等。在这种情况下，服务器可以将终端上传的数据从预设存储地址中删除。
- [81] 在一种实施方式中，在上述调用安全处理进程对终端上传的数据进行处理的步骤之后，还可以包括如下步骤：
- [82] 若检测到该数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与该终端对应的存储地址。
- [83] 比如，杀毒软件检测到终端上传的数据中携带的木马程序在杀毒软件的病毒库中有相应的记载以及对应的消除方法，那么杀毒软件就可以按照其记载的消除方法将该木马程序从终端上传的数据中消除。也就是说，若检测到终端上传的数据经过安全处理进程的处理后变为了安全数据，那么服务器可以将经过处理后的数据由预设存储地址存储到与该终端对应的存储地址中。
- [84] 在一种实施方式中，上述若检测到该数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与该终端对应的存储地址，还可以包括：若检测到终端上传的数据经过处理后变为了安全数据，则还可以进一步检测经过处理后的数据相比于终端原来上传的数据是否发生终端正常数据的缺失。
- [85] 若检测到经过处理后的数据相比于终端原来上传的数据，并没有发生终端正常的数据的缺失，而仅仅是终端原来上传的数据中的计算机病毒、木马或恶意程序被清除了，那么服务器可以将经过处理后的数据由预设存储地址存储到服务器中与该终端对应的存储地址中。

- [86] 若检测到经过处理后的数据相比于终端原来上传的数据，发生了终端正常数据的缺失。比如，终端向服务器上传的数据为五份文档文件，因这些文件中携带有计算机病毒，服务器对这五份文档文件进行了安全处理，清除了其中的计算机病毒，但是在处理过程中发现是这五份文档中的两份文档感染了计算机病毒，因此将这两份文档连同计算机病毒一起删除了。在这种情况下，由于经过处理后的数据相比于终端原来上传的数据发生了缺失（即由五份文档变为三份文档），因此服务器可以将剩余的三份文档由预设存储地址存储到与该终端对应的存储地址中，或者服务器也可以将剩余的三份文档也一并删除，等等，此处不做具体限定。
- [87] 本发明实施例提供一种数据存储的装置，包括：
- [88] 接收单元，用于从终端处接收上传的数据；
- [89] 保存单元，用于将所述数据保存至预设存储地址；
- [90] 扫描单元，用于调用安全防护进程对所述数据进行安全扫描，得到扫描结果；
- [91] 存储单元，用于若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [92] 在一种实施方式中，所述装置还包括：删除单元，用于若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除。
- [93] 在一种实施方式中，所述删除单元用于：若根据所述扫描结果确定出所述数据为不安全数据，则调用安全处理进程对所述数据进行处理。若检测到所述数据经过处理后未变为安全数据，则将所述数据从预设存储地址中删除。若检测到所述数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [94] 在一种实施方式中，所述装置还包括：提示单元，用于发送提示信息至所述终端，所述提示信息用于提示所述终端上传的数据为不安全数据，并被服务器删除。
- [95] 在一种实施方式中，所述存储单元，还可以用于：清空所述预设存储地址中的数据。
- [96] 在一种实施方式中，所述存储单元，还可以用于向所述终端发送用于提示所述

终端上传的数据为安全数据，并被存储到与所述终端对应的存储地址的信息。

[97] 请参阅图3，图3为本发明实施例提供的数据存储的装置的结构示意图。数据存储的装置300可以包括：接收单元301，保存单元302，扫描单元303，以及存储单元304。

[98] 接收单元301，用于从终端处接收上传的数据。

[99] 保存单元302，用于将所述数据保存至预设存储地址。

[100] 比如，接收单元301和保存单元302可以用于：

[101] 当服务器的接收单元301接收到终端上传的数据时，服务器的保存单元302可以先将该数据存储到一个指定的存储空间，即预设存储地址。

[102] 需要说明的是，预设存储地址是一个用于临时存储终端所上传的数据的存储空间，有别于服务器中与各个终端对应的存储空间。例如，在服务器中，甲终端对应的存储地址为第一存储地址，乙终端对应的存储地址为第二存储地址，等等。而预设存储地址是不同于第一存储地址以及第二存储地址的一个存储空间。例如当接收单元301接收到甲终端上传的数据时，服务器的保存单元302可以先将该数据保存在预先指定的预设存储地址，而不是立即保存到第一存储地址。之后，若接收单元301接收到乙终端上传的数据，那么保存单元302也是先将乙终端上传的数据保存到预设存储地址中，而不是第二存储地址。

[103] 扫描单元303，用于调用安全防护进程对所述数据进行安全扫描，得到扫描结果。

[104] 比如，在保存单元302将终端上传的数据保存到预设存储地址中之后，可以触发服务器的扫描单元303调用安全防护进程对终端上传的数据进行安全扫描，并得到扫描结果。例如，扫描单元303可以调用预设的杀毒软件对保存在预设存储地址中的数据进行安全扫描，并将扫描结果上报给服务器。

[105] 存储单元304，用于若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。

[106] 比如，在扫描单元303将扫描结果上报给服务器之后，服务器可以根据该扫描结果判断终端上传的数据是否为安全数据。

[107] 需要说明的是，当扫描单元303调用的安全防护进程在终端上传的数据中未检

测到计算机病毒、木马以及恶意程序等时，服务器会将终端上传的数据确定为安全数据。而如果扫描单元303调用的安全防护进程在终端上传的数据中检测到了计算机病毒、木马以及恶意程序等，那么服务器会将终端上传的数据确定为不安全数据，等等。

[108] 若服务器根据扫描单元303上报的扫描结果判断出终端上传的数据为安全数据，那么可以触发存储单元304将该数据由预设存储地址存储到服务器中与该终端对应的存储地址。例如，若服务器确定出甲终端上传的数据为安全数据，则存储单元304可以将甲终端上传的数据由预设存储地址转存到甲终端对应的第一存储地址中。

[109] 可以理解的是，在本发明实施例中，当接收单元301接收到终端上传的数据时，服务器并不是立即将该数据保存到服务器中与该终端对应的存储空间中，而是先由保存单元302将该数据保存在预设存储地址，并由扫描单元303对该数据进行安全扫描。只有当在该数据中没有扫描到计算机病毒、木马或恶意程序等时，才会由存储单元304将该数据由预设存储地址存储到服务器中与该终端对应的存储空间。通过这种方式，可以有效避免服务器因接收到包含计算机病毒、木马或恶意程序的数据，而对存储在服务器中的大量数据造成安全威胁。

[110] 请一并参阅图4，图4为本发明实施例提供的数据存储的装置的另一结构示意图。数据存储的装置300还可以包括：删除单元305以及提示单元306。

[111] 删除单元305，用于若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除。

[112] 比如，在扫描单元303将扫描结果上报给服务器之后，服务器根据该扫描结果判断出终端上传的数据为不安全的数据，在这种情况下，可以触发删除单元305将该终端本次上传的数据直接从预设存储地址中删除。

[113] 可以理解的是，在确定出终端上传的数据为不安全的数据时，通过将该数据直接从预设存储地址中删除，可以有效避免服务器中存储的数据遭受安全威胁。

[114] 在一种实施方式中，删除单元305可以用于：

[115] 若根据所述扫描结果确定出所述数据为不安全数据，则调用安全处理进程对所述数据进行处理；

- [116] 若检测到所述数据经过处理后未变为安全数据，则将所述数据从预设存储地址中删除；
- [117] 若检测到所述数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [118] 比如，服务器根据扫描单元303上报的扫描结果判断出终端上传的数据为不安全数据，那么此时服务器还可以调用安全处理进程对终端上传的数据进行处理。例如，安全防护进程检测到终端上传的数据中包含有木马程序。此时，服务器可以调用预设的杀毒软件，对该数据进行木马程序的消除处理。
- [119] 然而，由于杀毒软件的病毒库带有一定的局限性，杀毒软件无法对所有的计算机病毒、木马或恶意程序进行查杀。所以，若检测到终端上传的数据经过安全处理进程的处理后仍然为不安全的数据，也即安全处理进程无法消除终端上传的数据中携带的计算机病毒、木马或恶意程序等。在这种情况下，可以触发服务器的删除单元305将终端上传的数据从预设存储地址中删除。
- [120] 而如果杀毒软件检测到终端上传的数据中携带的木马程序在杀毒软件的病毒库中有相应的记载以及对应的消除方法，那么杀毒软件就可以按照其记载的方法将该木马程序从终端上传的数据中消除。也就是说，若检测到终端上传的数据经过安全处理进程的处理后变为了安全数据，那么服务器可以将经过处理后的数据由预设存储地址存储到与该终端对应的存储地址中。
- [121] 提示单元306，用于发送提示信息至所述终端，所述提示信息用于提示所述终端上传的数据为不安全数据，并被服务器删除。
- [122] 比如，在删除单元305将终端上传的数据从预设存储地址中删除之后，可以触发服务器的提示单元306向该终端发送一则提示信息，该提示信息用于提示该终端因其上传的数据中包含计算机病毒、木马或恶意程序等，而被服务器删除。
- [123] 本发明还提供一种数据存储的系统。请参阅图5，图5为本发明实施例提供的数据存储的系统的场景示意图。
- [124] 上述数据存储的系统可以包括一个或多个服务器，以及一个或多个终端。其中，该服务器可以集成如上述实施例所述的数据存储的装置。
- [125] 上述终端可以包括输入设备、输出设备、处理器以及存储器等。上述输入设备

可为物理按键。上述输出设备可为显示屏。上述处理器可以为中央处理器（CPU，Central Processing Unit）。上述存储器可以是高速RAM存储器，也可为非不稳定的存储器（non-volatile memory），例如磁盘存储器。上述输入设备、输出设备、处理器以及存储器通过总线连接。

[126] 比如，第一终端、第二终端以及第三终端分别向服务器上传了第一数据、第二数据以及第三数据。服务器在接收到这些数据后，会将这些数据先保存到指定的预设存储地址中。例如，服务器将第一数据保存到预设第一存储地址中，将第二数据保存到预设第二存储地址中，以及将第三数据保存到预设第三存储地址中。

[127] 然后，服务器调用安全防护进程在预设第一存储地址、预设第二存储地址以及预设第三存储地址中分别对第一数据、第二数据以及第三数据进行安全扫描，并得到对应的三份扫描结果。

[128] 接着，服务器根据获取到的扫描结果，判断第一数据、第二数据以及第三数据是否为安全数据。例如，服务器判断出第一数据和第二数据为不包含计算机病毒、木马或恶意程序的安全数据，而第三数据为不安全的数据。

[129] 基于上述判断结果，服务器可以将第一数据由预设第一存储地址存储到服务器中与第一终端对应的存储地址，将第二数据由预设第二存储地址存储到服务器中与第二终端对应的存储地址。而将第三数据从预设第三存储地址中删除。之后，服务器可以分别发送第一提示信息、第二提示信息以及第三提示信息到第一终端、第二终端以及第三终端。其中，第一提示信息和第二提示信息分别用于通知第一终端和第二终端其上传的数据为安全数据，并被存储到对应的存储地址中。而第三提示信息则用于通知第三终端其上传的数据为不安全数据，已被服务器删除，等等。

[130] 可以理解的是，在本发明实施例中，当接收到终端上传的数据时，服务器并不是立即将该数据保存到服务器中与该终端对应的存储空间中，而是先将该数据保存到预设存储地址中，并对该数据进行安全扫描。只有当在该数据中没有扫描到计算机病毒、木马或恶意程序等时，才会将该数据由预设存储地址存储到服务器中与该终端对应的存储地址。若在该数据中检测到计算机病毒、木马或

恶意程序等，则服务器可以将该数据直接删除。通过这种方式，可以有效避免服务器因接收到包含计算机病毒、木马或恶意程序的数据，而对存储在服务器中的大量数据造成安全威胁。

[131] 本发明实施例提供一种存储介质，其上存储有计算机程序，当所述计算机程序在计算机上执行时，使得所述计算机执行如本发明实施例提供的数据存储的方法。

[132] 本发明实施例还提供了一种服务器，其中可以集成如上实施例所提供的任一数据存储的装置。

[133] 请参考图6，其示出了本发明实施例所涉及的服务器400的结构示意图。

[134] 该服务器400可以包括一个或者一个以上处理核心的处理器401、一个或一个以上计算机可读存储介质的存储器402、通信单元403等部件。

[135] 处理器401是该服务器的控制中心，利用各种接口和线路连接整个服务器的各个部分，通过运行或执行存储在存储器402内的软件程序和/或模块，以及调用存储在存储器402内的数据，执行服务器的各种功能和处理数据，从而对服务器进行整体监控。处理器401可包括一个或多个处理核心。处理器401可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等。调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器401中。

[136] 存储器402可用于存储软件程序以及模块，处理器401通过运行存储在存储器402的软件程序以及模块，从而执行各种功能应用以及数据处理。

[137] 通信单元403可用于收发信息过程中，信号的接收和发送。特别地，通信单元403接收终端发送的信号，并将信号交由一个或者一个以上处理器401处理。同时，通信单元403将处理器401发出的反馈信号发送给终端。

[138] 服务器中的处理器401会按照如下的指令，将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器402中，并由处理器401来运行存储在存储器402中的应用程序，执行如下步骤：

[139] 从终端处接收上传的数据；

[140] 将所述数据保存至预设存储地址；

- [141] 调用安全防护进程对所述数据进行安全扫描，得到扫描结果；
- [142] 若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [143] 如图7所示，在一种实施方式中，服务器还可以包括电源404、输入单元405、以及显示单元406等部件。本领域技术人员可以理解，图6中示出的服务器结构并不构成对服务器的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：
- [144] 电源404可以通过电源管理系统与处理器401逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源404还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。
- [145] 输入单元405可用于接收输入的数字或字符信息，以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。
- [146] 显示单元406可用于显示由用户输入的信息或提供给用户的信息以及服务器的各种图形用户接口，这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元406可包括显示面板。在一种实施方式中，显示单元可以采用液晶显示器（LCD，Liquid Crystal Display）、有机发光二极管（OLED，Organic Light-Emitting Diode）等形式来配置显示面板。
- [147] 在一种实施方式中，在执行得到扫描结果的步骤之后，处理器401可以执行如下步骤：若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除。
- [148] 在一种实施方式中，处理器401在执行所述若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除的步骤时，可以包括如下步骤：若根据所述扫描结果确定出所述数据为不安全数据，则调用安全处理进程对所述数据进行处理。若检测到所述数据经过处理后未变为安全数据，则将所述数据从预设存储地址中删除。
- [149] 在一种实施方式中，在执行所述调用安全处理进程对所述数据进行处理步骤之后，处理器401还可以执行如下步骤：若检测到所述数据经过处理后变为安全

数据，则将经过处理后的数据由预设存储地址存储到服务器中与所述终端对应的存储地址。

[150] 在一种实施方式中，在执行所述将所述数据从预设存储地址中删除的步骤之后，处理器401还可以执行如下步骤：发送提示信息至所述终端，所述提示信息用于提示所述终端上传的数据为不安全数据，并被服务器删除。

[151] 在一种实施方式中，在执行所述将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址的步骤之后，处理器401还可以执行如下步骤：清空所述预设存储地址中的数据。

[152] 在一种实施方式中，在执行所述将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址的步骤之后，处理器401还可以执行如下步骤：向所述终端发送用于提示所述终端上传的数据为安全数据，并被存储到与所述终端对应的存储地址的信息。

[153] 在上述实施例，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见上文针对数据存储的方法的详细描述，此处不再赘述。

[154] 本发明实施例提供的所述数据存储的装置与上文实施例中的数据存储的方法属于同一构思，在所述数据存储的装置上可以运行所述数据存储的方法实施例中提供的任一方法，其实现过程详见所述数据存储的方法实施例，此处不再赘述。

[155] 需要说明的是，对本发明实施例所述数据存储的方法而言，本领域普通技术人员可以理解实现本发明实施例所述数据存储的方法的全部或部分流程，是可以通过计算机程序来控制相关的硬件来完成，所述计算机程序可存储于一计算机可读取存储介质中，如存储在存储器中，并被至少一个处理器执行，在执行过程中可包括如所述数据存储的方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储器（ROM，Read Only Memory）、随机存取记忆体（RAM，Random Access Memory）等。

[156] 对本发明实施例的所述数据存储的装置而言，其各功能模块可以集成在一个处理芯片中，也可以是各个模块单独物理存在，也可以两个或两个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件

功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中，所述存储介质譬如为只读存储器，磁盘或光盘等。

- [157] 以上对本发明实施例所提供的一种数据存储的方法、装置、存储介质、服务器以及系统进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权利要求书

- [权利要求 1] 一种数据存储的方法，其中，所述方法包括：
- 从终端处接收上传的数据；
- 将所述数据保存至预设存储地址；
- 调用安全防护进程对所述数据进行安全扫描，得到扫描结果；
- 若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [权利要求 2] 根据权利要求1所述的数据存储的方法，其中，在得到扫描结果的步骤之后，还包括：
- 若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除。
- [权利要求 3] 根据权利要求2所述的数据存储的方法，其中，所述若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除，包括：
- 若根据所述扫描结果确定出所述数据为不安全数据，则调用安全处理进程对所述数据进行处理；
- 若检测到所述数据经过处理后未变为安全数据，则将所述数据从预设存储地址中删除。
- [权利要求 4] 根据权利要求3所述的数据存储的方法，其中，在调用安全处理进程对所述数据进行处理步骤之后，还包括：
- 若检测到所述数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [权利要求 5] 根据权利要求4所述的数据存储的方法，其中，在将所述数据从预设存储地址中删除的步骤之后，还包括：
- 发送提示信息至所述终端，所述提示信息用于提示所述终端上传的数据为不安全数据，并被服务器删除。
- [权利要求 6] 根据权利要求1所述的数据存储的方法，其中，在将所述数据由预

设存储地址存储到服务器中与所述终端对应的存储地址的步骤之后，还包括：

清空所述预设存储地址中的数据。

[权利要求 7]

根据权利要求1所述的数据存储的方法，其中，在将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址的步骤之后，还包括：

向所述终端发送用于提示所述终端上传的数据为安全数据，并被存储到与所述终端对应的存储地址的信息。

[权利要求 8]

一种数据存储的装置，其中，所述装置包括：

接收单元，用于从终端处接收上传的数据；

保存单元，用于将所述数据保存至预设存储地址；

扫描单元，用于调用安全防护进程对所述数据进行安全扫描，得到扫描结果；

存储单元，用于若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。

[权利要求 9]

根据权利要求8所述的数据存储的装置，其中，所述装置还包括：删除单元，用于若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除。

[权利要求 10]

根据权利要求9所述的数据存储的装置，其中，所述删除单元用于：

若根据所述扫描结果确定出所述数据为不安全数据，则调用安全处理进程对所述数据进行处理；

若检测到所述数据经过处理后未变为安全数据，则将所述数据从预设存储地址中删除；

若检测到所述数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与所述终端对应的存储地址。

- [权利要求 11] 根据权利要求10所述的数据存储的装置，其中，所述装置还包括：
- 提示单元，用于发送提示信息至所述终端，所述提示信息用于提示所述终端上传的数据为不安全数据，并被服务器删除。
- [权利要求 12] 根据权利要求8所述的数据存储的装置，其中，所述存储单元，用于：
- 清空所述预设存储地址中的数据。
- [权利要求 13] 一种存储介质，其上存储有计算机程序，其中，当所述计算机程序在计算机上执行时，使得所述计算机执行如权利要求1至7中任一项所述的数据存储的方法。
- [权利要求 14] 一种服务器，包括存储器，处理器，其中，所述处理器通过调用所述存储器中存储的计算机程序，用于执行如下步骤：
- 从终端处接收上传的数据；
- 将所述数据保存至预设存储地址；
- 调用安全防护进程对所述数据进行安全扫描，得到扫描结果；
- 若根据所述扫描结果确定出所述数据为安全数据，则将所述数据由预设存储地址存储到服务器中与所述终端对应的存储地址。
- [权利要求 15] 根据权利要求14所述的服务器，其中，所述处理器执行如下步骤：
- 若根据所述扫描结果确定出所述数据为不安全数据，则将所述数据从预设存储地址中删除。
- [权利要求 16] 根据权利要求15所述的服务器，其中，所述处理器执行如下步骤：
- 若根据所述扫描结果确定出所述数据为不安全数据，则调用安全处理进程对所述数据进行处理；
- 若检测到所述数据经过处理后未变为安全数据，则将所述数据从预设存储地址中删除。
- [权利要求 17] 根据权利要求16所述的服务器，其中，所述处理器执行如下步骤

:

若检测到所述数据经过处理后变为安全数据，则将经过处理后的数据由预设存储地址存储到服务器中与所述终端对应的存储地址。

[权利要求 18] 根据权利要求17所述的服务器，其中，所述处理器执行如下步骤

:

送提示信息至所述终端，所述提示信息用于提示所述终端上传的数据为不安全数据，并被服务器删除。

[权利要求 19] 根据权利要求14所述的服务器，其中，所述处理器执行如下步骤

:

清空所述预设存储地址中的数据。

[权利要求 20] 一种数据存储的系统，包括服务器和终端，其中，所述服务器包括如权利要求8至12中任一项所述的数据存储的装置。

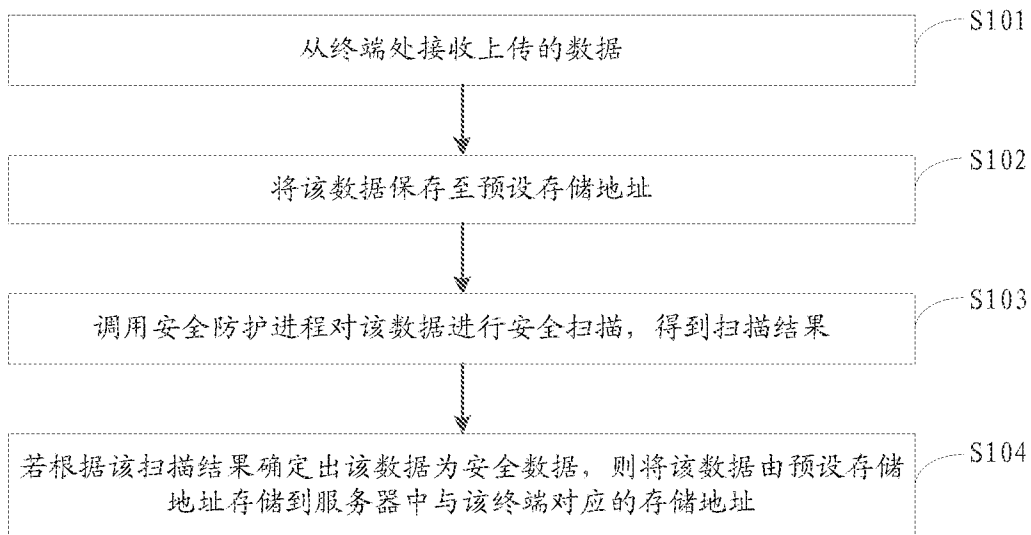


图 1

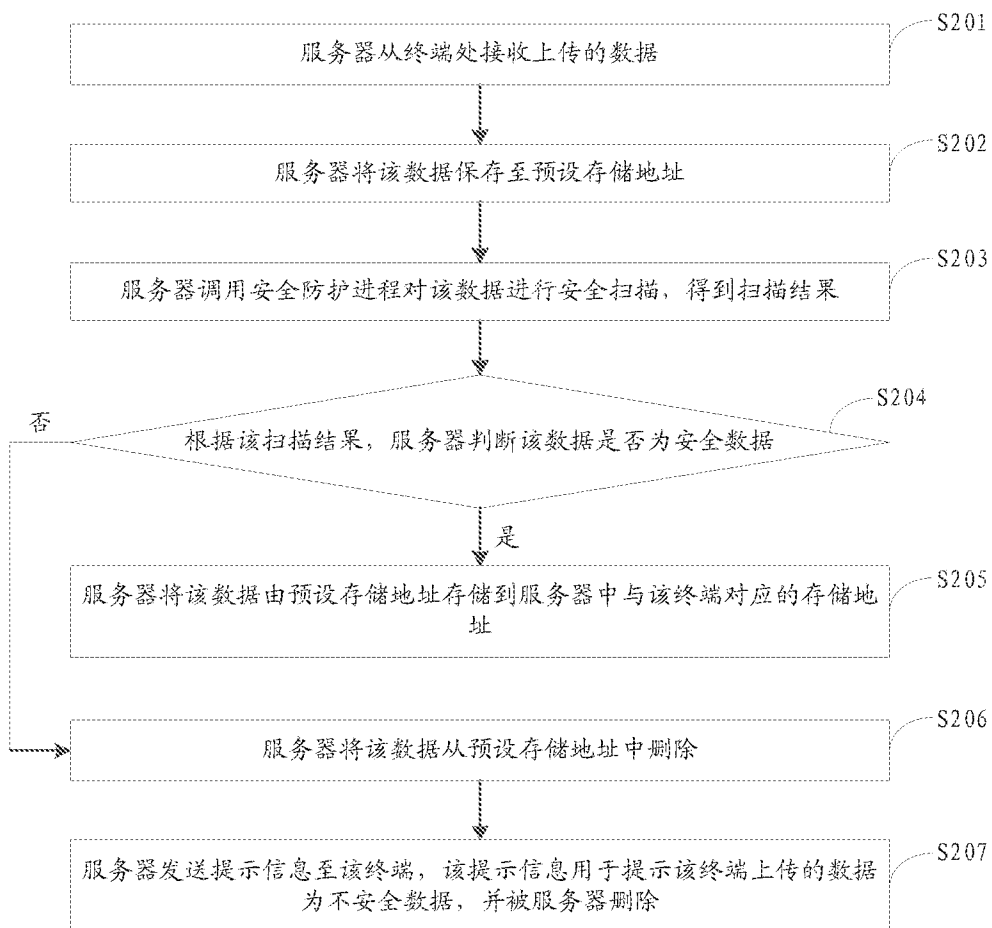


图 2

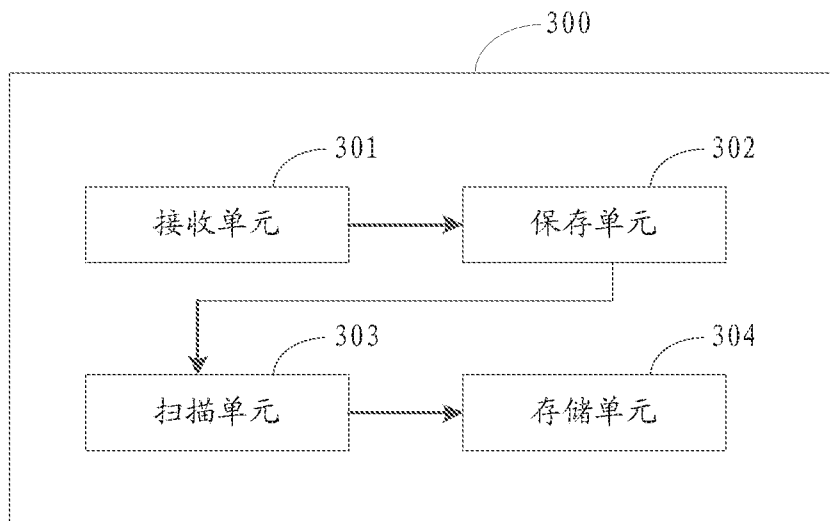


图 3

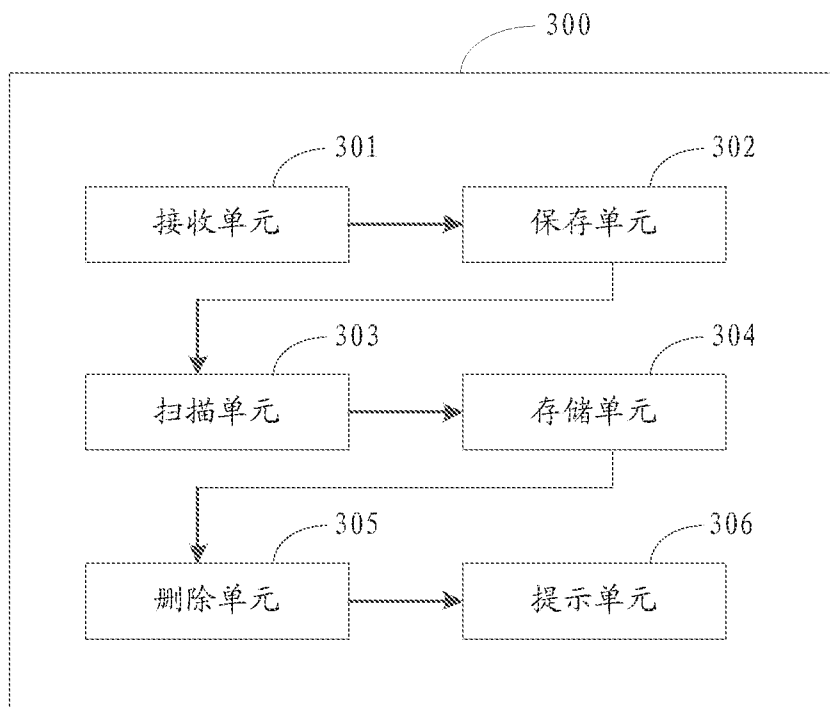


图 4

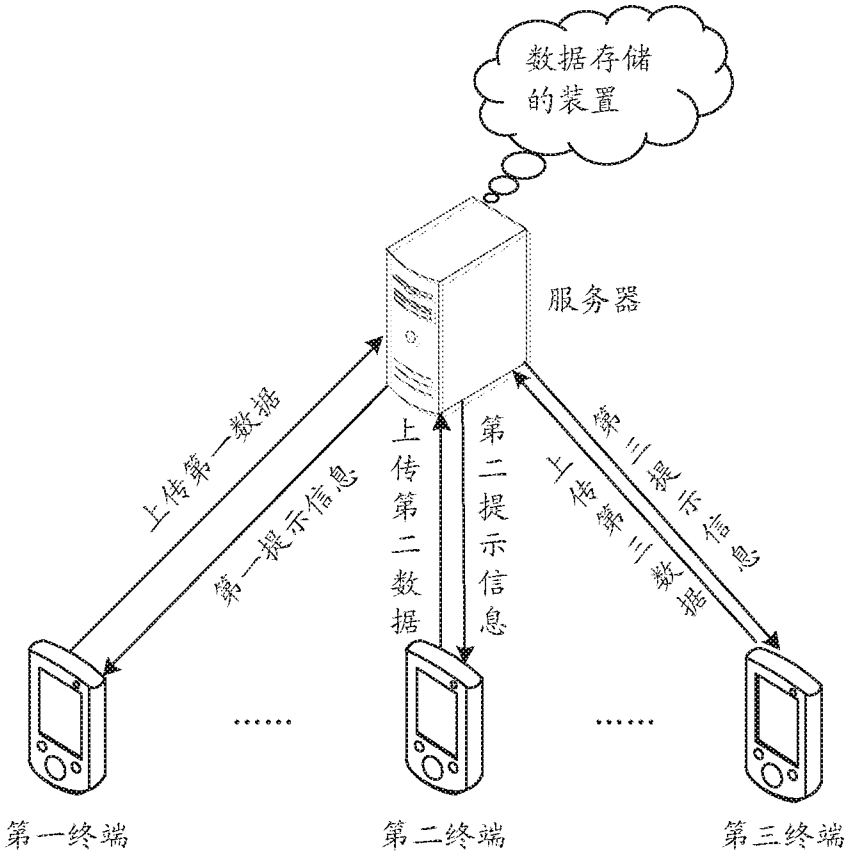


图 5

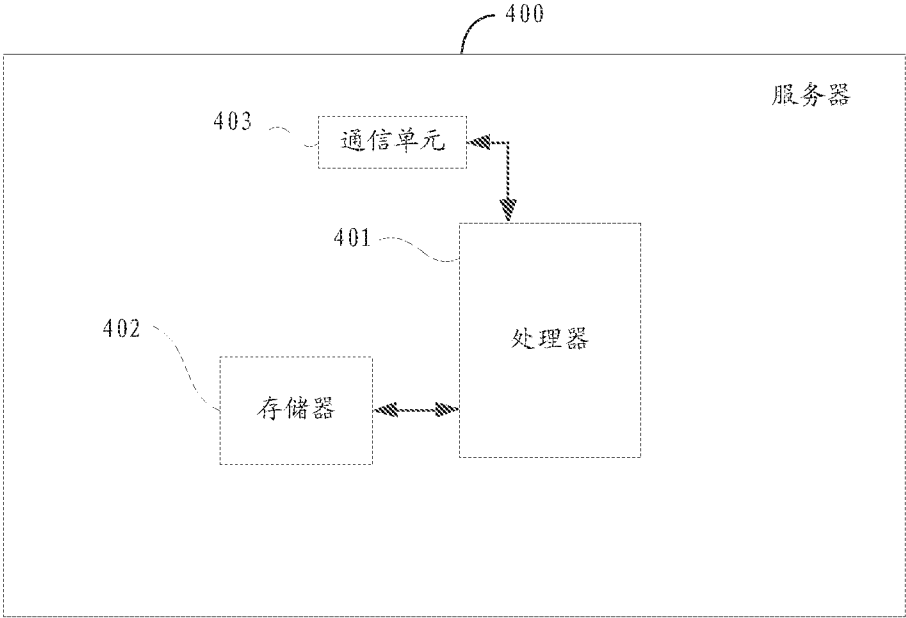


图 6

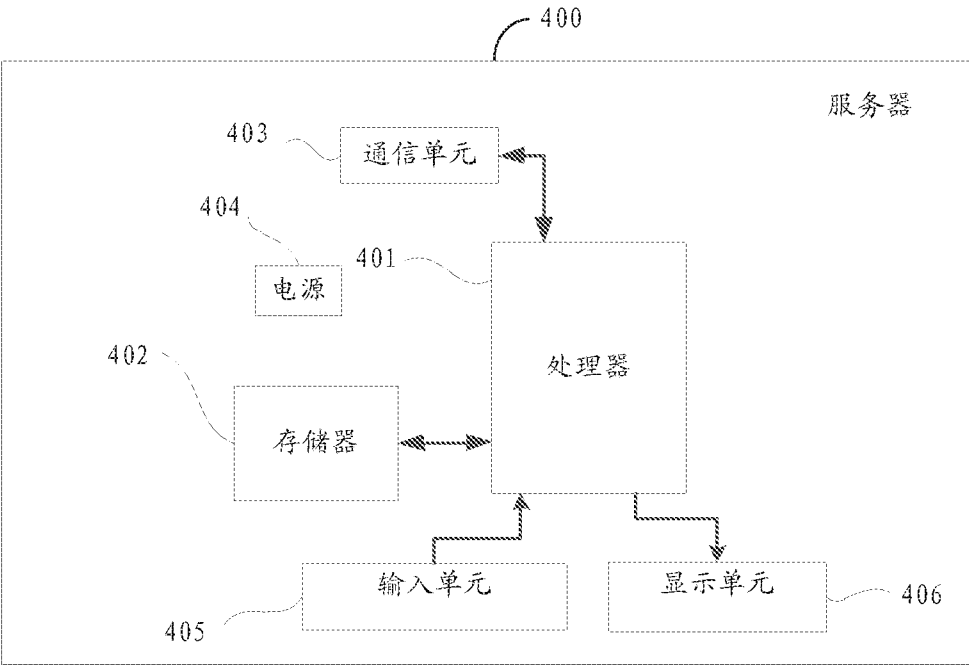


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/095618

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, GOOGLE: 数据, 存储, 云端, 服务器, 终端, 上传, 备份, 扫描, 存储地址, 安全数据, 木马, 病毒, data, storage, cloud, terminal, upload, backup, scan, safe, trojan, virus

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106503556 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.) 15 March 2017 (15.03.2017), description, paragraphs [0029]-[0037], [0043]-[0063], [0077]-[0101] and [0114]	1-20
X	CN 104023070 A (DU, Haiyang) 03 September 2014 (03.09.2014), description, paragraphs [0044]-[0046]	1-20
A	CN 105323261 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 10 February 2016 (10.02.2016), entire document	1-20
A	CN 104410683 A (SICHUAN CINGHOO TECHNOLOGY CO., LTD.) 11 March 2015 (11.03.2015), entire document	1-20
A	US 2012084341 A1 (MICROSOFT CORPORATION) 05 April 2012 (05.04.2012), entire document	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 10 October 2017	Date of mailing of the international search report 01 November 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer MA, Jintao Telephone No. (86-10) 62414067

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/095618

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106503556 A	15 March 2017	None	
CN 104023070 A	03 September 2014	CN 104023070 B	15 February 2017
CN 105323261 A	10 February 2016	None	
CN 104410683 A	11 March 2015	None	
US 2012084341 A1	05 April 2012	WO 2012050700 A2	19 April 2012
		EP 2622502 A2	07 August 2013
		US 9560130 B2	31 January 2017
		CN 102413168 A	11 April 2012
		CN 102413168 B	26 October 2016
		US 2017169066 A1	15 June 2017

国际检索报告

国际申请号

PCT/CN2017/095618

A. 主题的分类

G06F 21/56(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, WPI, EPODOC, CNKI, GOOGLE: 数据, 存储, 云端, 服务器, 终端, 上传, 备份, 扫描, 存储地址, 安全数据, 木马, 病毒, data, storage, cloud, terminal, upload, backup, scan, safe, trojan, virus

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 106503556 A (广东欧珀移动通信有限公司) 2017年 3月 15日 (2017 - 03 - 15) 说明书第[0029]-[0037]、[0043]-[0063]、[0077]-[0101]、[0114]段	1-20
X	CN 104023070 A (杜海洋) 2014年 9月 3日 (2014 - 09 - 03) 说明书第[0044]-[0046]段	1-20
A	CN 105323261 A (北京奇虎科技有限公司 等) 2016年 2月 10日 (2016 - 02 - 10) 全文	1-20
A	CN 104410683 A (四川神琥科技有限公司) 2015年 3月 11日 (2015 - 03 - 11) 全文	1-20
A	US 2012084341 A1 (MICROSOFT CORPORATION) 2012年 4月 5日 (2012 - 04 - 05) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2017年 10月 10日

国际检索报告邮寄日期

2017年 11月 1日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

马晋涛

传真号 (86-10)62019451

电话号码 (86-10)62414067

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/095618

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106503556	A	2017年 3月 15日	无			
CN	104023070	A	2014年 9月 3日	CN	104023070	B	2017年 2月 15日
CN	105323261	A	2016年 2月 10日	无			
CN	104410683	A	2015年 3月 11日	无			
US	2012084341	A1	2012年 4月 5日	WO	2012050700	A2	2012年 4月 19日
				EP	2622502	A2	2013年 8月 7日
				US	9560130	B2	2017年 1月 31日
				CN	102413168	A	2012年 4月 11日
				CN	102413168	B	2016年 10月 26日
				US	2017169066	A1	2017年 6月 15日

表 PCT/ISA/210 (同族专利附件) (2009年7月)