(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
2024 年 2 月 29 日 (29.02.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/040977 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2023/087180

(22) 国际申请日: 2023 年 4 月 8 日 (08.04.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202211018624.7 2022年8月24日 (24.08.2022) CN

(71) 申请人: 华 为 技 术 有 限 公 司 **(HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中 国 广 东 省 深 圳 市 龙 岗 区 坂 田 华 为 总 部 办 公 楼, Guangdong 518129 (CN)。

(72) 发明人: 刘 遵 一 **(LIU, Zunyi)**; 中 国 广 东 省 深 圳 市 龙 岗 区 坂 田 华 为 总 部 办 公 楼, Guangdong 518129 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,

(54) **Title:** VIRUS DETECTION METHOD AND APPARATUS, ELECTRONIC DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 一种病毒检测方法、装置、电子设备及存储介质

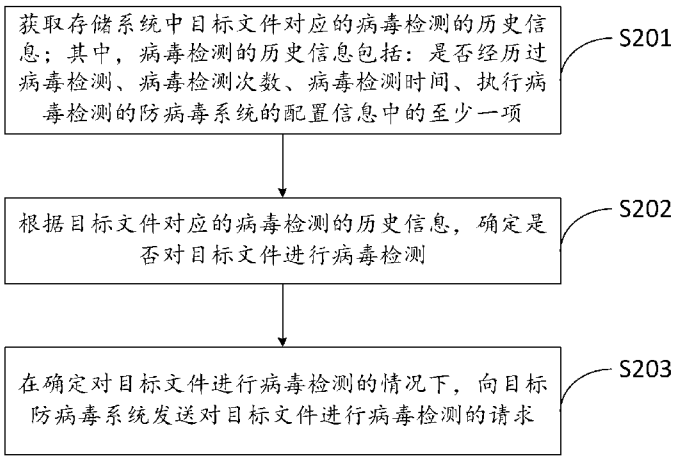

图 2

(57) **Abstract:** The present application relates to a virus detection method and apparatus, an electronic device, and a storage medium. The method comprises: acquiring historical information of virus detection corresponding to a target file in a storage system; according to the historical information of virus detection corresponding to the target file, determining whether to carry out virus detection on the target file; if it is determined that virus detection is to be carried out on the target file, sending a request for carrying out virus detection on the target file to a target anti-virus system. In this way, whether virus detection is to be carried out on a target file is determined according to historical information of virus detection corresponding to the target file, and on the premise of ensuring data security, virus detection can be prevented from being repeatedly carried out on file content already subjected to virus detection, so that the network bandwidth overhead is saved, the virus detection time is saved, and the virus detection efficiency and the read-write performance of storage systems are improved.

WO 2024/040977 A1

[见续页]

CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明:
— 关于申请人有权要求在先申请的优先权(细则4.17(iii))

本国际公布:
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本申请涉及一种病毒检测方法、装置、电子设备及存储介质。其中，该方法可以包括：获取存储系统中目标文件对应的病毒检测的历史信息；根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测；在确定对所述目标文件进行病毒检测的情况下，向目标防病毒系统发送对所述目标文件进行病毒检测的请求；这样，根据目标文件对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经进行过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率及存储系统的读写性能。

一种病毒检测方法、装置、电子设备及存储介质

技术领域

本申请涉及计算机安全领域，尤其涉及一种病毒检测方法、装置、电子设备及存储介质。

背景技术

防病毒（Anti Virus，AV）技术是一种保护用户数据安全的技术，具有实时监控、防范病毒、扫描病毒或清除病毒等功能，维护用户计算机资源的安全。网络连接存储（Network Attached Storage，NAS）防病毒作为NAS存储系统中的一个增值特性，通常与防病毒软件协作保护NAS存储系统中文件的数据安全，从而有效防止NAS存储系统的文件被病毒感染篡改，保护整个NAS存储系统的可靠运行。

然而，现有对NAS防病毒的方式会消耗大量的网络带宽，以及消耗大量的时间，效率较低。

发明内容

有鉴于此，提出了一种病毒检测方法、装置、电子设备及存储介质。

第一方面，本申请的实施例提供了一种病毒检测方法，所述方法包括：获取存储系统中目标文件对应的病毒检测的历史信息；其中，所述病毒检测的历史信息包括：是否经历过病毒检测、病毒检测次数、病毒检测时间、执行病毒检测的防病毒系统的配置信息中的至少一项；根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测；在确定对所述目标文件进行病毒检测的情况下，向目标防病毒系统发送对所述目标文件进行病毒检测的请求。

基于上述技术方案，目标文件对应的病毒检测的历史信息可以表征目标文件的内容所经历的病毒检测的相关信息；根据目标文件对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经进行过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第一方面，在所述第一方面的第一种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括所述目标文件元数据中的病毒检测的历史信息，和/或，索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；其中，所述索引库中包括至少一个文件指纹及所述至少一个文件指纹对应的病毒检测的历史信息，所述至少一个文件指纹与所述存储系统中的一个或多个文件相关联，所述至少一个文件指纹对应的病毒检测的历史信息包括与所述至少一个文件指纹相关联的各文件对应的病毒检测的历史信息中最新的历史信息。

根据第一方面或第一方面的第一种可能的实现方式，在所述第一方面的第二种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息；所述获取目标文件对应的病毒检测的历史信息，包括：在所述目标文件元数据中，读取所述目标文件对应的病毒检测的历史信息。

基于上述技术方案，在一个文件经过病毒检测且确认无病毒后，若该文件内容没有发生变化，则该文件内容仍旧是安全的，则可以不对该文件重复进行病毒检测；因此，读取目标文件元数据中的病毒检测的历史信息，快速获取目标文件对应的病毒检测的历史信息，进而根据目标文件元数据中的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保

证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第一方面或第一方面的第一种可能的实现方式，在所述第一方面的第三种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述获取目标文件对应的病毒检测的历史信息，包括：确定所述目标文件的目标文件指纹；根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息。

基于上述技术方案，目标文件指纹与存储系统中一个或多个文件相关联，即该一个或多个文件的内容完全相同，若通过病毒检测确认该一个或多个文件中的任一文件是安全的，则其他文件的内容也可以认为是安全的，则可以不对其他文件重复进行病毒检测；因此，在索引库中查询目标文件指纹对应的病毒检测的历史信息，根据目标文件指纹对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第一方面的第二种可能的实现方式，在所述第一方面的第四种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息，和，所述索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测，包括：在所述目标文件元数据中的病毒检测的历史信息不满足第一预设条件的情况下，确定所述目标文件的目标文件指纹；根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息；在所述目标文件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定对所述目标文件进行病毒检测。

基于上述技术方案，根据目标文件元数据中的病毒检测的历史信息和索引库中目标文件指纹对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第一方面或第一方面上述各种可能的实现方式，在所述第一方面的第五种可能的实现方式中，所述方法还包括：获取所述目标防病毒系统反馈的对所述目标文件进行病毒检测的结果；根据所述病毒检测的结果，更新所述目标文件对应的病毒检测的历史信息。

基于上述技术方案，根据病毒检测结果更新目标文件对应的病毒检测的历史信息，可以保证目标文件对应的病毒检测的历史信息为最新的病毒检测的历史信息，以便下一次触发病毒检测任务时，基于最新的病毒检测的历史信息确定是否对目标文件进行病毒检测。

根据第一方面的第四种可能的实现方式，在所述第一方面的第六种可能的实现方式中，所述方法还包括：在所述目标文件指纹对应的病毒检测的历史信息满足第二预设条件的情况下，确定不对所述目标文件进行病毒检测，并更新所述目标文件元数据中的病毒检测的历史信息。

基于上述技术方案，目标文件指纹对应的病毒检测的历史信息满足第二预设条件表明目标文件指纹对应的文件内容经历过病毒检测且没有病毒，即目标文件的内容经历过病毒检测

且没有病毒，则可以更新目标文件元数据中的病毒检测的历史信息，从而保证目标文件元数据中的病毒检测的历史信息为最新的病毒检测的历史信息，以便下一次触发病毒检测任务时通过目标文件元数据中的病毒检测的历史信息快速确定是否需要对目标文件进行病毒检测，或者是否需要获取目标文件指纹。

第二方面，本申请的实施例提供了一种病毒检测装置，所述装置包括：获取模块，用于获取存储系统中目标文件对应的病毒检测的历史信息；其中，所述病毒检测的历史信息包括：是否经历过病毒检测、病毒检测次数、病毒检测时间、执行病毒检测的防病毒系统的配置信息中的至少一项；确定模块，用于根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测；请求模块，用于在确定对所述目标文件进行病毒检测的情况下，向目标防病毒系统发送对所述目标文件进行病毒检测的请求。

基于上述技术方案，目标文件对应的病毒检测的历史信息可以表征目标文件的内容所经历的病毒检测的相关信息；根据目标文件对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经进行过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第二方面，在所述第二方面的第一种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括所述目标文件元数据中的病毒检测的历史信息，和/或，索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；其中，所述索引库中包括至少一个文件指纹及所述至少一个文件指纹对应的病毒检测的历史信息，所述至少一个文件指纹与所述存储系统中的一个或多个文件相关联，所述至少一个文件指纹对应的病毒检测的历史信息包括与所述至少一个文件指纹相关联的各文件对应的病毒检测的历史信息中最新的历史信息。

根据第二方面或第二方面的第一种可能的实现方式，在所述第二方面的第二种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息；所述获取模块，还用于在所述目标文件元数据中，读取所述目标文件对应的病毒检测的历史信息。

基于上述技术方案，在一个文件经过病毒检测且确认无病毒后，若该文件内容没有发生变化，则该文件内容仍旧是安全的，则可以不对该文件重复进行病毒检测；因此，读取目标文件元数据中的病毒检测的历史信息，快速获取目标文件对应的病毒检测的历史信息，根据目标文件元数据中的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第二方面或第二方面的第一种可能的实现方式，在所述第二方面的第三种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述获取模块，还用于：确定所述目标文件的目标文件指纹；根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息。

基于上述技术方案，目标文件指纹与存储系统中一个或多个文件相关联，即该一个或多个文件的内容完全相同，若通过病毒检测确认该一个或多个文件中的任一文件是安全的，则其他文件的内容也可以认为是安全的，则可以不对其他文件重复进行病毒检测；因此，在索引库中查询目标文件指纹对应的病毒检测的历史信息，根据目标文件指纹对应的病毒检测的

历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第二方面的第二种可能的实现方式，在所述第二方面的第四种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息，和，所述索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述确定模块，还用于：在所述目标文件元数据中的病毒检测的历史信息不满足第一预设条件的情况下，确定所述目标文件的目标文件指纹；根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息；在所述目标文件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定对所述目标文件进行病毒检测。

基于上述技术方案，根据目标文件元数据中的病毒检测的历史信息和索引库中目标文件指纹对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

根据第二方面或第二方面上述各种可能的实现方式，在所述第二方面的第五种可能的实现方式中，所述装置还包括：结果反馈模块，用于获取所述目标防病毒系统反馈的对所述目标文件进行病毒检测的结果；更新模块，用于根据所述病毒检测的结果，更新所述目标文件对应的病毒检测的历史信息。

基于上述技术方案，根据病毒检测结果更新目标文件对应的病毒检测的历史信息，可以保证目标文件对应的病毒检测的历史信息为最新的病毒检测的历史信息，以便下一次触发病毒检测任务时，基于最新的病毒检测的历史信息确定是否对目标文件进行病毒检测。

根据第二方面的第四种可能的实现方式，在所述第二方面的第六种可能的实现方式中，所述装置还包括：元数据更新模块，在所述目标文件指纹对应的病毒检测的历史信息满足第二预设条件的情况下，确定不对所述目标文件进行病毒检测，并更新所述目标文件元数据中的病毒检测的历史信息。

基于上述技术方案，目标文件指纹对应的病毒检测的历史信息满足第二预设条件表明目标文件指纹对应的文件内容经历过病毒检测且没有病毒，即目标文件的内容经历过病毒检测且没有病毒，则可以更新目标文件元数据中的病毒检测的历史信息，从而保证目标文件元数据中的病毒检测的历史信息为最新的病毒检测的历史信息，以便下一次触发病毒检测任务时通过目标文件元数据中的病毒检测的历史信息快速确定是否需要对目标文件进行病毒检测，或者是否需要获取目标文件指纹。

第三方面，本申请的实施例提供了一种电子设备，包括：处理器；用于存储处理器可执行指令的存储器；其中，所述处理器被配置为执行所述指令时实现第一方面或第一方面的一种或几种的病毒检测方法。

第四方面，本申请的实施例提供了一种计算机可读存储介质，其上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现第一方面或第一方面的一种或几种的病毒检测方法。

第五方面，本申请的实施例提供了一种计算机程序产品，当所述计算机程序产品在计算机上运行时，使得所述计算机执行上述第一方面或第一方面的一种或几种的病毒检测方法。

上述第三方面至第五方面的技术效果，可参见上述第一方面或第二方面。

根据下面参考附图对示例性实施例的详细说明，本申请的其它特征及方面将变得清楚。

附图说明

包含在说明书中并且构成说明书的一部分的附图与说明书一起示出了本申请的示例性实施例、特征和方面，并且用于解释本申请的原理。

图 1 示出了根据本申请一实施例的病毒检测方法的一种适用场景的示意图。

图 2 示出根据本申请一实施例的一种病毒检测方法的流程图。

图 3 示出根据本申请一实施例的一种索引库的示意图。

图 4 示出根据本申请一实施例的文件指纹 1 对应的病毒检测的历史信息的示意图。

图 5 示出根据本申请一实施例的一种病毒检测方法的流程图。

图 6 示出根据本申请一实施例的一种病毒检测方法的流程图。

图 7 示出根据本申请一实施例的一种病毒检测方法的流程图。

图 8 示出根据本申请一实施例的一种病毒检测装置的结构示意图。

图 9 示出根据本申请一实施例的一种电子设备的结构示意图。

具体实施方式

以下将参考附图详细说明本申请的各种示例性实施例、特征和方面。附图中相同的附图标记表示功能相同或相似的元件。尽管在附图中示出了实施例的各种方面，但是除非特别指出，不必按比例绘制附图。

在本说明书中描述的参考 “一个实施例”或“一些实施例”等意味着在本申请的一个或多个实施例中包括结合该实施例描述的特定特征、结构或特点。由此，在本说明书中的不同之处出现的语句“在一个实施例中”、“在一些实施例中”、“在其他一些实施例中”、“在另外一些实施例中”等不是必然都参考相同的实施例，而是意味着“一个或多个但不是所有的实施例”，除非是以其他方式另外特别强调。术语“包括”、“包含”、“具有”及它们的变形都意味着“包括但不限于”，除非是以其他方式另外特别强调。在这里专用的词“示例性”意为“用作例子、实施例或说明性”。这里作为“示例性”所说明的任何实施例不必解释为优于或好于其它实施例。另外，为了更好的说明本申请，在下文的具体实施方式中给出了众多的具体细节。本领域技术人员应当理解，没有某些具体细节，本申请同样可以实施。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：包括单独存在 A，同时存在 A 和 B，以及单独存在 B 的情况，其中 A，B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a，b，或 c 中的至少一项（个），可以表示：a，b，c，a-b，a-c，b-c，或 a-b-c，其中 a，b，c 可以是单个，也可以是多个。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范

围。

下面首先对本申请实施例所适应的应用场景进行举例说明。

图 1 示出了根据本申请一实施例的病毒检测方法的一种适用场景的示意图。如图 1 所示，该场景中可以包括存储系统 10、防病毒系统 20；其中，存储系统 10 可以与防病毒系统 20 通过有线或无线网络连接。

其中，存储系统 10 中可以包括防病毒单元，用于向防病毒系统 20 发送病毒检测请求，触发病毒检测；其中，病毒检测请求中可以包括目标文件的存储路径或者目标文件的内容。示例性地，存储系统 10 可以为 NAS 存储系统；NAS 存储系统中可以包括 1-n 个文件系统（File System，FS），用于存储和组织数据，以便根据文件路径信息确定对应的文件。在一些示例中，管理员可以预先通过图形管理界面或命令行视图（command-line interface，CLI）配置存储系统 10 中的防病毒功能；在需要对存储系统 10 中的文件进行病毒检测时，防病毒单元可以向防病毒系统 20 发送病毒检测请求。

其中，防病毒系统 20 用于对文件进行病毒检测以及杀毒处理。防病毒系统 20 可以外置于存储系统 10，也可以部署在存储系统 10 内部，对此不作限定。在一些示例中，防病毒系统 20 可以配置有防病毒服务器（AV Server），也可以称为防病毒引擎（AV Engine），可以通过安装的防病毒软件执行病毒检测；如果存储系统 10 发送的是目标文件的路径，则由防病毒服务器通过文件访问协议，例如，网络文件系统（Network File System，NFS）协议、SMB 协议、通用 Internet 文件系统（Common Internet File System，CIFS）协议、互联网内容适配协议（Internet Content Adaptation Protocol，ICAP）等，根据目标文件的路径从存储系统 10 中获取目标文件的内容，从而进行病毒检测；如果存储系统 10 发送的是目标文件的内容，则由防病毒服务器直接对目标文件的内容进行病毒检测，从而判断是否有病毒。在另一些示例中，防病毒系统 20 还可以配置有防病毒代理（Av Agent），从而为防病毒服务器获取存储系统 10 所发送的信息提供代理服务。

示例性地，该场景中还可以包括客户端 30，例如，可以为服务器信息块（Server Message Block，SMB）客户机（client）；用户可以通过客户端 30 向存储系统 10 发送操作访问请求，从而对存储系统 10 中的文件进行打开、写入、保存、关系或读取等操作。

相关技术中，在用户对存储系统 10 中的目标文件进行操作访问时，触发对该目标文件进行在线病毒检测任务，也称实时扫描（On-Access Scanning）；或者管理员可以配置定期（例如，在凌晨等空闲时间段）对存储系统 10 中文件进行全局或局部防病毒扫描，触发存储系统 10 主动对目标文件进行后台病毒检测任务。在触发对目标文件进行在线病毒检测任务或触发存储系统 10 主动对目标文件进行后台病毒检测任务，存储系统 10 都要向防病毒系统 20 发送对目标文件进行病毒检测的请求，防病毒系统 20 接收到病毒检测请求后，获取目标文件的内容（直接接收存储系统 10 发送的目标文件的内容，或者，根据存储系统 10 发送的目标文件的路径获取目标文件的内容），并对所获取的目标文件的内容进行病毒检测。由于存储系统中通常存储有海量文件，在触发病毒检测任务时，存储系统 10 中的目标文件的内容均需要传输到防病毒系统 20，从而消耗大量的网络输入输出（input output，IO）传输带宽及时间，效率较低。此外，触发在线病毒检测任务时，在防病毒系统 20 完成对目标文件的病毒检测前，用户是无法对目标文件打开访问的，从而对存储系统 10 的读写性能造成很大的影响。

考虑到在存储系统 10 存储的海量的文件中有大量的重复文件，例如，数据拷贝、快照、克隆、复制等灾备特性拷贝的文件，这些重复文件的内容完全相同，若通过病毒检测确认重复文件中的一个文件是安全的，重复文件中其他文件的内容也可以认为是安全的，则可以不

对重复文件中其他文件重复进行病毒检测；此外，在一个文件经过病毒检测确认无病毒后，若该文件内容没有发生变化，则该文件内容仍旧是安全的，则可以不对该文件重复进行病毒检测；基于此，本申请实施例提供了一种病毒检测方法（详细描述参见下文），可以在保证数据安全的前提下，跳过已经进行过病毒检测的文件内容，避免将重复的文件内容发送给防病毒系统进行病毒检测，从而节约了网络带宽开销，节省了病毒检测的时间，提高了病毒检测的效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统10的读写性能。

需要说明的是，本申请实施例描述的上述应用场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，针对其他相似的或新的场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。例如，本申请所述病毒检测方法对于其他存储系统，如基于对象的存储系统、分布式文件系统（Distributed File System，HDFS）、大数据存储系统等存储系统，同样适用。

下面以上述图1所示的场景为例，对本申请实施例提供的病毒检测方法进行详细说明。

图2示出根据本申请一实施例的一种病毒检测方法的流程图。示例性地，该方法可以由上述图1中防病毒单元执行。如图2所示，该方法可以包括以下步骤：

S201、获取存储系统中目标文件对应的病毒检测的历史信息。

示例性地，可以在触发病毒检测任务时，获取存储系统中目标文件对应的病毒检测的历史信息；例如，可以在用户对存储系统中的目标文件进行操作访问时，触发对目标文件进行在线病毒检测任务，防病毒单元获取目标文件对应的病毒检测的历史信息；再例如，可以在触发存储系统主动对目标文件进行后台病毒检测任务时，防病毒单元获取目标文件对应的病毒检测的历史信息。作为一个示例，存储系统可以为上述图1所示的存储系统10。

目标文件对应的病毒检测的历史信息可以表征目标文件的内容所经历的病毒检测的相关信息；其中，病毒检测的历史信息可以包括：是否经历过病毒检测、病毒检测次数、病毒检测时间、执行病毒检测的防病毒系统的配置信息中的至少一项。

其中，是否经历过病毒检测表示一个文件的内容是否经历过病毒检测；例如，经历过病毒检测表示一个文件的内容在当前时刻之前经历过病毒检测且确定没有病毒，未经历过病毒检测表示一个文件的内容在当前时刻之前未经历过病毒检测。病毒检测次数表示一个文件的内容经历病毒检测的次数。病毒检测时间表示一个文件的内容经历病毒检测的时间，例如，可以为最新病毒检测时间，即该文件的内容最新一次经历病毒检测的时间。执行病毒检测的防病毒系统的配置信息表示一个文件的内容经历病毒检测时执行病毒检测的防病毒系统的配置信息，例如，可以为执行最新一次病毒检测的防病毒系统的配置信息；示例性地，执行病毒检测的防病毒系统可以包括杀毒软件，防病毒系统的配置信息可以是该杀毒软件的版本号。

示例性地，当一个文件的内容发生变化时，如在一个文件中写入新的内容或删除部分内容，或者，一个文件的内容经过病毒检测确定存在病毒时，可以将该文件对应的病毒检测的历史信息更新为默认值；作为一个示例，默认值可以包括未经历过病毒检测、病毒检测次数为0、病毒检测时间为空、或执行病毒检测的防病毒系统的配置信息为空中的一项或多项。

在一种可能的实现方式中，目标文件对应的病毒检测的历史信息包括目标文件元数据中的病毒检测的历史信息。即目标文件元数据中可以记载有目标文件的内容是否经历过病毒检测、目标文件的内容经历病毒检测的次数、目标文件的内容经历病毒检测的时间、目标文件的内容经历病毒检测时执行病毒检测的防病毒系统的配置信息中的至少一项。示例性地，防病毒单元可以在目标文件的元数据中读取目标文件对应的病毒检测的历史信息。

作为一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容是否经历过病毒检测为例。例如，当目标文件的内容经历过病毒检测，并确认没有病毒后，可以在目标文件元数据中记录“已扫描”的标记，从而表征目标文件的内容经历过病毒检测；如果目标文件的内容发生变化，存在被病毒侵入的风险，则在目标文件元数据中清除该“已扫描”的标记，从而表征修改后的目标文件的内容未经历过病毒检测。

作为另一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容经历病毒检测的时间为例。例如，当目标文件的内容经历病毒检测，并确认没有病毒后，可以在目标文件元数据中记录该病毒检测的时间；若目标文件的内容再次经历病毒检测且确认没有病毒，则可以根据该次经历病毒检测的时间更新目标文件元数据中所记载的病毒检测的时间。

作为另一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容经历病毒检测时执行病毒检测的防病毒系统的配置信息为例。例如，当目标文件的内容经历过病毒检测，并确认没有病毒后，可以在目标文件元数据中记录执行此次病毒检测的杀毒软件的版本号；若目标文件的内容再次经历病毒检测且确认没有病毒后，则可以根据执行该次病毒检测的杀毒软件的版本号更新目标文件元数据中所记载的杀毒软件的版本号。

作为另一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容经历病毒检测的次数为例。例如，目标文件的内容每进行一次病毒检测，并确认没有病毒后，可以将目标文件对应的病毒检测的历史信息中记录的病毒检测次数增加 1。

作为另一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容是否经历过病毒检测和目标文件的内容经历病毒检测的时间为例。当目标文件进行过病毒检测，并确认没有病毒后，可以在目标文件元数据中记录“已扫描”的标记以及本次病毒检测的时间。

作为另一个示例，目标文件元数据中的病毒检测的历史信息可以包括目标文件的内容是否经历过病毒检测、目标文件的内容经历病毒检测的时间、及目标文件的内容经历病毒检测时执行病毒检测的防病毒系统的配置信息；当目标文件进行过病毒检测，并确认没有病毒后，可以在目标文件元数据中记录“已扫描”的标记、本次病毒检测的时间以及执行本次病毒检测的防病毒系统的配置信息。

在一种可能的实现方式中，目标文件对应的病毒检测的历史信息可以包括索引库中与目标文件的文件指纹对应的病毒检测的历史信息；示例性地，防病毒单元可以在索引库中查询与目标文件的目标文件指纹对应的病毒检测的历史信息。

其中，索引库中包括至少一个文件指纹及该至少一个文件指纹对应的病毒检测的历史信息，该至少一个文件指纹与存储系统中的一个或多个文件相关联，该至少一个文件指纹对应的病毒检测的历史信息包括与该至少一个文件指纹相关联的各文件对应的病毒检测的历史信息中最新的历史信息。

作为一个示例，对于目标文件，当在存储系统中创建目标文件并写入内容后，关闭目标文件时，可以根据目标文件的内容计算目标文件的文件指纹；其中，文件指纹可以通过现有计算文件指纹的方式得到。示例性地，可以将目标文件的文件指纹记录在目标文件的元数据中。这样，遍历存储系统中各文件，从而可以得到各文件的文件指纹；进而汇总各文件的文件指纹，可以得到多个不同的文件指纹；其中，内容相同的文件的文件指纹相同，内容不同的文件的文件指纹不同。进一步地，针对任一文件指纹，汇总与该文件指纹相关联的各文件对应的病毒检测的历史信息，从而将相关联的各文件对应的病毒检测的历史信息中最新的历史信息作为该文件指纹对应的病毒检测的历史信息；最后在索引库中插入以文件指纹为键

（key）的索引记录（即文件指纹对应的病毒检测的历史信息），从而建立索引库；索引库中可以记载有是否经历过病毒检测、病毒检测的次数、病毒检测的时间、执行病毒检测的防病毒系统的配置信息中的至少一项。

举例来说，图 3 示出根据本申请一实施例的一种索引库的示意图，如图 3 所示，索引库中可以包括多个文件指纹，分别为文件指纹 1、文件指纹 2、文件指纹 3…文件指纹 n；其中，每个文件指纹对应的病毒检测的历史信息可以包括该文件指纹对应的文件内容是否经历过病毒检测、该文件指纹对应的文件内容经历病毒检测的时间、该文件指纹对应的文件内容经历病毒检测时执行病毒检测的杀毒软件的版本号。例如，图 3 中文件指纹 1 对应的病毒检测的历史信息包括：经历过病毒检测、病毒检测时间为 T1、执行病毒检测的杀毒软件版本号为 P1；再例如，文件指纹 3 对应的病毒检测的历史信息包括：未经历过病毒检测、病毒检测时间为空、执行病毒检测的杀毒软件版本号为空。

示例性地，如果存储系统中某一文件的内容发生变化，例如，对某一文件的内容进行增加、删除、改写等操作后，该文件的文件指纹会发生变化，则重新计算该文件的文件指纹，再例如，若某一文件的内容经过病毒检测且确定存在病毒，进行杀毒处理后该文件的内容也会发生变化，则重新计算该文件的文件指纹；或者，如果存储系统中有新建的文件，则可以计算该新建文件的文件指纹。进而可以更新索引库中该最新的文件指纹对应的病毒检测的历史信息；若在索引库中没有查询到与该最新的文件指纹，可以在索引库中插入以该最新的文件指纹为 key 的索引记录。

示例性地，针对任一文件指纹，可以根据该文件指纹相关联的各文件的内容是否经历过病毒检测的信息，确定该文件指纹对应的是否经历过病毒检测的信息，若相关联的各文件中任一文件的内容经历过病毒检测，即最新的是否经历过病毒检测的信息为经历过病毒检测，则该文件指纹对应的病毒检测的历史信息中包括经历过病毒检测的信息；例如，可以在索引库中该文件指纹对应的索引记录中添加“已扫描”的标记；若相关联的各文件的内容均未经历过病毒检测，则该文件指纹对应的病毒检测的历史信息中包括未经历过病毒检测的信息。示例性地，针对任一文件指纹，可以在该文件指纹相关联的各文件对应的病毒检测时间中选取其中最新的病毒检测时间，作为该文件指纹对应的病毒检测时间。示例性地，针对任一文件指纹，可以在该文件指纹相关联的各文件对应的执行病毒检测的防病毒系统的配置信息中选取其中最新的防病毒系统的配置信息，作为该文件指纹对应的执行病毒检测的防病毒系统的配置信息；例如，可以将该文件指纹相关联的各文件对应的执行病毒检测的杀毒软件版本号中最新的杀毒软件版本号，作为该文件指纹对应的执行病毒检测的杀毒软件版本号。

举例来说，图 4 示出根据本申请一实施例的文件指纹 1 对应的病毒检测的历史信息的示意图，如图 4 所示，存储系统中文件 B 及文件 C 为对文件 A 进行数据拷贝、快照、克隆或复制等操作所得到的新文件，文件 A 的内容、文件 B 的内容及文件 C 的内容均相同，文件 A、文件 B 及文件 C 的文件指纹相同，均为文件指纹 1，即，文件指纹 1 与存储系统中文件 A、文件 B、文件 C 相关联。文件 A 对应的病毒检测的历史信息包括文件 A 的内容经历过病毒检测、病毒检测时间为 2022 年 1 月 1 日 15 时、杀毒软件版本号为 p1；文件 B 对应的病毒检测的历史信息为文件 B 的内容经历过病毒检测、病毒检测时间为 2022 年 1 月 1 日 13 时、杀毒软件版本号为 p2；文件 C 对应的病毒检测的历史信息为文件 C 的内容未经历过病毒检测、病毒检测时间为空、杀毒软件版本号为空。由于文件 A 和文件 B 的内容经历过病毒检测，即最新的是否经历过病毒检测的信息为经历过病毒检测，则可以确定文件指纹 1 对应的病毒检测历史信息包括经历过病毒检测的信息；文件 A 对应的病毒检测时间晚于文件 B 对应的病毒检测时

间，即最新的病毒检测时间为文件 A 对应的病毒检测时间，则可以确定文件指纹 1 对应的病毒检测时间为 2022 年 1 月 1 日 15 时；文件 A 对应的杀毒软件版本号 p1 相对于文件 B 对应的杀毒软件版本号 p2 更新，即最新的执行病毒检测的杀毒软件版本号为 p1，则可以确定文件指纹 1 对应的杀毒软件版本号为 p1。

在一种可能的实现方式中，目标文件对应的病毒检测的历史信息包括目标文件元数据中的病毒检测的历史信息及索引库中与目标文件的文件指纹对应的病毒检测的历史信息。

其中，目标文件元数据中的病毒检测的历史信息与索引库中与目标文件的文件指纹对应的病毒检测的历史信息的类型可以相同，也可以不同，对此不作限定。例如，目标文件元数据中的病毒检测的历史信息可以包括是否经历过病毒检测，目标文件的文件指纹对应的病毒检测的历史信息可以包括病毒检测时间；再例如，目标文件元数据中的病毒检测的历史信息可以包括是否经历过病毒检测，目标文件的文件指纹对应的病毒检测的历史信息可以包括是否经历过病毒检测。

S202、根据目标文件对应的病毒检测的历史信息，确定是否对目标文件进行病毒检测。

示例性地，可以在目标文件对应的病毒检测的历史信息满足预设条件的情况下，确定不对目标文件进行病毒检测；在目标文件对应的病毒检测的历史信息不满足预设条件的情况下，确定对目标文件进行病毒检测。

作为一个示例，以目标文件对应的病毒检测的历史信息包括是否经历过病毒检测为例，对应的预设条件可以包括目标文件的内容经历过病毒检测。例如，如果目标文件对应的病毒检测的历史信息中存在“已扫描”的标记，表明目标文件的内容经历过病毒检测，则确定不对目标文件进行病毒检测；如果目标文件对应的病毒检测的历史信息中没有“已扫描”的标记，则确定对目标文件进行病毒检测。

作为另一个示例，以目标文件对应的病毒检测的历史信息包括病毒检测的时间为例，对应的预设条件可以包括目标文件对应的病毒检测的历史信息中病毒检测时间与当前时刻的间隔未超过预设时间间隔。如果目标文件对应的病毒检测的历史信息中病毒检测时间与当前时刻的间隔未超过预设时间间隔，确定不对目标文件进行病毒检测；如果目标文件对应的病毒检测的历史信息中病毒检测时间与当前时刻的间隔超过了预设时间间隔，目标文件的内容存在感染病毒的风险，则确定对目标文件进行病毒检测；其中，预设时间间隔的数值可以根据需要进行设定，对此不作限定。

作为另一个示例，以目标文件对应的病毒检测的历史信息包括病毒检测的次数为例，对应的预设条件可以包括目标文件对应的病毒检测的历史信息中病毒检测的次数未超过预设检测次数。如果目标文件对应的病毒检测的历史信息中病毒检测次数达到了预设检测次数，确定不对目标文件进行病毒检测；如果目标文件对应的病毒检测的历史信息中病毒检测次数未达到预设检测次数，则确定对目标文件进行病毒检测；其中，预设检测次数的数值可以根据需要进行设定，对此不作限定。

作为另一个示例，以目标文件对应的病毒检测的历史信息包括执行病毒检测的防病毒系统的配置信息为例，对应的预设条件可以包括执行病毒检测的防病毒系统的配置信息与目标防病毒系统（即当前执行病毒检测的防病毒系统）的配置信息相同。例如，如果目标文件对应的病毒检测的历史信息中杀毒软件的版本号与当前执行病毒检测的杀毒软件的版本号相同，可以跳过目标文件，不对目标文件进行病毒检测；如果目标文件对应的病毒检测的历史信息中杀毒软件的版本号与当前执行病毒检测的杀毒软件的版本号不同（例如杀毒软件进行了更新导致杀毒软件的版本号发生了变化），则确定对目标文件进行病毒检测。

作为另一个示例，以目标文件对应的病毒检测的历史信息包括是否经历过病毒检测和病毒检测时间为例，对应的预设条件可以为目标文件的内容经历过病毒检测、及目标文件对应的病毒检测的历史信息中病毒检测时间与当前时刻的间隔未超过预设时间间隔。例如，如果目标文件对应的病毒检测的历史信息中存在“已扫描”的标记且目标文件对应的病毒检测的历史信息中病毒检测时间与当前时刻的间隔未超过预设时间间隔，则确定不对目标文件进行病毒检测；否则，确定对目标文件进行病毒检测。

作为另一个示例，以目标文件对应的病毒检测的历史信息包括是否经历过病毒检测、病毒检测时间和执行病毒检测的防病毒系统的配置信息为例；对应的预设条件可以为目标文件的内容经历过病毒检测、目标文件对应的病毒检测的历史信息中病毒检测时间与当前时刻的间隔未超过预设时间间隔及执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同。例如，如果目标文件对应的病毒检测的历史信息中存在“已扫描”的标记、目标文件对应的病毒检测的历史信息中病毒检测时间与当前时刻的间隔未超过预设时间间隔、且目标文件对应的病毒检测的历史信息中杀毒软件的版本号与当前执行病毒检测的杀毒软件的版本号相同，则确定不对目标文件进行病毒检测；否则，确定对目标文件进行病毒检测。

S203、在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求。

示例性地，存储系统可以与一个或多个防病毒系统进行无线或有线连接，可以在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求。作为一个示例，目标防病毒系统可以为上述图 1 中的防病毒系统 20。

示例性地，病毒检测的请求还可以包括目标文件的路径或者目标文件的内容，以便目标防病毒系统对目标文件进行病毒检测。例如，在确定对目标文件进行病毒检测的情况下，防病毒单元可以将目标文件的路径发送给目标防病毒系统，目标防病毒系统基于目标文件的路径通过文件访问协议从存储系统中获取目标文件的内容后再进行病毒检测，从而判断目标文件的内容中是否有病毒；再例如，防病毒单元可以将目标文件的内容发送给目标防病毒系统器，目标防病毒系统直接对接收到的目标文件的内容进行病毒检测，从而判断目标文件的内容中是否有病毒。

示例性地，在确定不对目标文件进行病毒检测的情况下，则可以跳过对目标文件的病毒检测。例如，在触发在线病毒检测任务时，若确定不对目标文件进行病毒检测，则可以直接允许用户对目标文件进行操作。

在一种可能的实现方式中，在执行完上述步骤 S203 后，还可以获取目标防病毒系统反馈的对目标文件进行病毒检测的结果；根据病毒检测的结果，更新目标文件对应的病毒检测的历史信息。以便下一次触发病毒检测任务时，基于最新的病毒检测的历史信息确定是否对目标文件进行病毒检测。

作为一个示例，若目标文件对应的病毒检测的历史信息中没有“已扫描”的标记；如果目标防病毒系统对目标文件进行病毒检测后，目标防病毒系统确认目标文件没有病毒，则可以向防病毒单元反馈目标文件没有病毒；防病毒单元可以在目标文件对应的病毒检测的历史信息添加“已扫描”的标记。若目标文件对应的病毒检测的历史信息中有“已扫描”的标记；如果目标防病毒系统对目标文件进行病毒检测后，目标防病毒系统确认目标文件有病毒，则可以对目标文件进行杀毒（例如，该目标文件中部分或全部内容进行删除、隔离等处理），并向防病毒单元反馈目标文件有病毒，由于杀毒处理后目标文件的内容发生变化，防病毒单元可以在杀毒后的目标文件对应的病毒检测的历史信息中删除“已扫描”的标记。

作为另一个示例，如果目标防病毒系统对目标文件进行病毒检测后，目标防病毒系统确认目标文件没有病毒，则可以向防病毒单元反馈目标文件没有病毒及本次病毒检测时间，防病毒单元可以将目标文件对应的病毒检测的历史信息中的病毒检测时间更新为此次病毒检测时间。如果目标防病毒系统对目标文件进行病毒检测后，目标防病毒系统确认目标文件有病毒，则可以对目标文件进行杀毒，并向防病毒单元反馈目标文件有病毒，防病毒单元可以将目标文件对应的病毒检测的历史信息中的病毒检测时间更新为默认值。

作为另一个示例，如果目标防病毒系统对目标文件进行病毒检测后，目标防病毒系统确认目标文件没有病毒，则可以向防病毒单元反馈目标文件没有病毒及执行本次病毒检测的杀毒软件的版本号；防病毒单元可以将目标文件对应的病毒检测的历史信息中的执行病毒检测的杀毒软件的版本号更新为本次病毒检测的杀毒软件的版本号。如果目标防病毒系统对目标文件进行病毒检测后，目标防病毒系统确认目标文件有病毒，则可以对目标文件进行杀毒，并向防病毒单元反馈目标文件有病毒，防病毒单元可以将目标文件对应的病毒检测的历史信息中的执行病毒检测的杀毒软件的版本号更新为默认值。

本申请实施例中，目标文件对应的病毒检测的历史信息可以表征目标文件的内容所经历的病毒检测的相关信息；根据目标文件对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经进行过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

下面以目标文件对应的病毒检测的历史信息包括目标文件元数据中的病毒检测的历史信息为例，对本申请实施例中病毒检测方法进行说明。

图 5 示出根据本申请一实施例的一种病毒检测方法的流程图。示例性地，示例性地，该方法可以由上述图 1 中防病毒单元执行。如图 5 所示，该病毒检测方法包括：

S501、在目标文件元数据中，读取目标文件对应的病毒检测的历史信息。

其中，目标文件元数据的具体说明可参照上述图 2 中步骤 201 中相关表述。

S502、根据目标文件对应的病毒检测的历史信息，确定是否对目标文件进行病毒检测。

示例性地，可以在目标文件元数据中的病毒检测的历史信息满足预设条件的情况下，确定不对目标文件进行病毒检测；在目标文件对应的病毒检测的历史信息不满足预设条件的情况下，确定对目标文件进行病毒检测。

该步骤的具体实现过程可参照上述图 2 中步骤 S202 中的相关表述，在此不再赘述。

S503、在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求。

该步骤的具体实现过程可参照上述图 2 中步骤 S203 的相关表述，在此不再赘述。

在一种可能的实现方式中，在执行完上述步骤 S503 后，还可以获取目标防病毒系统反馈的对目标文件进行病毒检测的结果；并根据病毒检测的结果，更新目标文件元数据中的病毒检测的历史信息。示例性地，在目标防病毒系统对目标文件进行病毒检测后，可以向防病毒单元反馈目标文件是否存在病毒、该次病毒检测的时间或目标防病毒系统的配置信息中的一项或多项，防病毒单元根据反馈的信息在目标文件元数据中更新病毒检测的历史信息。

这样，通过上述步骤 S501-S503，读取目标文件元数据中的病毒检测的历史信息，快速获取目标文件对应的病毒检测的历史信息；考虑到在一个文件经过病毒检测且确认无病毒后，若该文件内容没有发生变化，则该文件内容仍旧是安全的，则可以不对该文件重复进行病毒检测；因此，根据目标文件元数据中的病毒检测的历史信息确定是否对目标文件进行病毒检

测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

作为一个示例，以目标文件元数据中的病毒检测的历史信息包括该目标文件的内容是否经历过病毒检测为例。可以在目标文件元数据中读取目标文件的内容是否经历过病毒检测，例如，可以读取目标文件元数据中是否有“已扫描”的标记，从而判断目标文件的内容是否经历过病毒检测。如果目标文件元数据中没有“已扫描”的标记，代表目标文件的内容没有经历过病毒检测，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果目标文件元数据中存在“已扫描”的标记，代表目标文件的内容已经进行过病毒检测并确认没有病毒，则确定不对目标文件进行病毒检测。

作为另一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容所经历的病毒检测时间为例。可以在目标文件元数据中读取目标文件的内容所经历的病毒检测时间，如果目标文件的内容所经历的病毒检测时间与当前时刻的间隔超过了预设时间间隔，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果目标文件的内容所经历的病毒检测时间与当前时刻的间隔未超过预设时间间隔，则可以确定不对目标文件进行病毒检测。

作为另一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容经历病毒检测时执行病毒检测的防病毒系统的配置信息为例。可以在目标文件元数据中读取执行病毒检测的防病毒系统的配置信息，如果执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息不同，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，则可以确定不对目标文件进行病毒检测。

作为另一个示例，以目标文件元数据中的病毒检测的历史信息包括目标文件的内容是否经历过病毒检测、目标文件的内容经历病毒检测时间和目标文件的内容经历病毒检测时执行病毒检测的防病毒系统的配置信息为例。可以在目标文件元数据中读取目标文件是否经历过病毒检测、病毒检测时间和执行病毒检测的防病毒系统的配置信息；例如，可以读取目标文件元数据中是否有“已扫描”的标记、目标文件的内容最新一次经历病毒检测的时间、执行最新一次病毒检测的防病毒系统的配置信息，如果目标文件元数据中有“已扫描”的标记、目标文件的内容最新一次经历病毒检测的时间与当前时刻的间隔未超过预设时间间隔、且执行最新一次病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，则确定不对目标文件进行病毒检测；否则，确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。

下面以目标文件对应的病毒检测的历史信息包括索引库中与目标文件的文件指纹对应的病毒检测的历史信息为例，对本申请实施例中病毒检测方法进行说明。

图 6 示出根据本申请一实施例的一种病毒检测方法的流程图。示例性地，示例性地，该方法可以由上述图 1 中防病毒单元执行。如图 6 所示，该病毒检测方法包括：

S601、确定目标文件的目标文件指纹；

作为一个示例，可以在目标文件元数据中，读取目标文件的目标文件指纹；

作为另一个示例，可以根据目标文件中的内容，计算目标文件的目标文件指纹。其中，计算目标文件指纹的方式可以采用现有技术，此处不再赘述；例如，可以采用哈希码生成目标文件指纹。

S602、根据目标文件指纹，在索引库中选取目标文件指纹对应的病毒检测的历史信息。

其中，索引库的具体说明可参照上述图 2 中步骤 201 中相关表述。

示例性地，可以以目标文件指纹为 key 在索引库中进行查询，获取与目标文件指纹对应的病毒检测的历史信息。

示例性地，如果以目标文件指纹为 key 在索引库中进行查询，没有查询到目标文件指纹对应的病毒检测的历史信息，则可以在索引库中插入以目标文件指纹为 key 的索引记录，该索引记录中目标文件指纹对应的病毒检测的历史信息设置为默认值。

S603、根据目标文件指纹对应的病毒检测的历史信息，确定是否对目标文件进行病毒检测。

示例性地，可以在目标文件指纹对应的病毒检测的历史信息满足预设条件的情况下，确定不对目标文件进行病毒检测；在目标文件指纹对应的病毒检测的历史信息不满足预设条件的情况下，确定对目标文件进行病毒检测。

该步骤的具体实现过程可参照上述图 2 中步骤 S202 的相关表述，在此不再赘述。

S604、在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求。

该步骤的具体实现过程可参照上述图 2 中步骤 S203 的相关表述，在此不再赘述。

在一种可能的实现方式中，在执行完上述步骤 S604 后，还可以获取目标防病毒系统反馈的对目标文件进行病毒检测的结果；并根据病毒检测的结果，更新索引库中与目标文件的文件指纹对应的病毒检测的历史信息。示例性地，在目标防病毒系统对目标文件进行病毒检测后，可以向防病毒单元反馈目标文件是否存在病毒、该次病毒检测的时间或目标防病毒系统的配置信息中的一项或多项，防病毒单元根据反馈的信息更新索引库中目标文件指纹对应的病毒检测的历史信息。

这样，通过上述步骤 S601-S604，在索引库中查询目标文件指纹对应的病毒检测的历史信息；考虑到目标文件指纹与存储系统中一个或多个文件相关联，即该一个或多个文件的内容完全相同，若通过病毒检测确认该一个或多个文件中的任一文件是安全的，则其他文件的内容也可以认为是安全的，则可以不对其他文件重复进行病毒检测；因此，根据目标文件指纹对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

作为一个示例，以索引库中与目标文件指纹对应的病毒检测的历史信息包括是否经历过病毒检测为例；例如，可以以目标文件指纹为 key 在索引库中进行查询，获取目标文件指纹对应的病毒检测的历史信息中是否存在“已扫描”的标记，从而判断目标文件的内容是否经历过病毒检测。如果索引库中目标文件指纹对应的病毒检测的历史信息中没有“已扫描”的标记，则代表目标文件的内容没有经历过病毒检测，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果索引库中目标文件指纹对应的病毒检测的历史信息中存在“已扫描”的标记，代表目标文件的内容已经进行过病毒检测并确认没有病毒，则确定不对目标文件进行病毒检测。

作为一个示例，以索引库中与目标文件指纹对应的病毒检测的历史信息包括病毒检测的时间为例；例如，可以以目标文件指纹为 key 在索引库中进行查询，获取目标文件指纹对应病毒检测的时间；如果目标文件指纹对应的病毒检测时间与当前时刻的间隔超过了预设时间

间隔，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果目标文件指纹对应的病毒检测时间与当前时刻的间隔未超过预设时间间隔，则确定不对目标文件进行病毒检测。

作为另一个示例，以索引库中与目标文件指纹对应的病毒检测的历史信息包括执行病毒检测的防病毒系统的配置信息为例；例如，可以以目标文件指纹为 key 在索引库中进行查询，获取目标文件指纹对应的执行病毒检测的防病毒系统的配置信息，如果目标文件指纹对应的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息不同，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果目标文件指纹对应的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，则可以确定不对目标文件进行病毒检测。

作为另一个示例，以索引库中与目标文件指纹对应的病毒检测的历史信息包括是否经历过病毒检测、病毒检测时间和执行病毒检测的防病毒系统的配置信息为例；例如，可以以目标文件指纹为 key 在索引库中进行查询，获取目标文件指纹对应的病毒检测的历史信息中是否存在“已扫描”的标记、目标文件指纹对应的病毒检测时间和目标文件指纹对应的执行病毒检测的防病毒系统的配置信息；如果目标文件指纹对应的病毒检测的历史信息中有“已扫描”的标记、目标文件指纹对应的病毒检测时间与当前时刻的间隔未超过预设时间间隔、且目标文件指纹对应的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，则确定不对目标文件进行病毒检测；否则，确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。

下面以目标文件对应的病毒检测的历史信息包括目标文件元数据中的病毒检测的历史信息，和，索引库中与目标文件的文件指纹对应的病毒检测的历史信息为例，对本申请实施例中病毒检测方法进行说明。

图 7 示出根据本申请一实施例的一种病毒检测方法的流程图。示例性地，该方法可以由上述图 1 中防病毒单元执行。如图 7 所示，该病毒检测方法包括：

S701、在目标文件元数据中，读取目标文件对应的病毒检测的历史信息。

该步骤与上述图 5 中步骤 S501 相同，在此不再赘述。

S702、在目标文件元数据中的病毒检测的历史信息不满足第一预设条件的情况下，确定目标文件的目标文件指纹。

其中，确定目标文件的目标文件指纹的方式可参照上述图 6 中步骤 S601 中相关表述。

在一种可能的实现方式中，还可以在目标文件元数据中的病毒检测的历史信息满足第一预设条件的情况下，确定目标文件的目标文件指纹。例如，目标文件可能长时间未经历病毒检测，为了进一步保证数据安全，仍可以在元数据中记载有“已扫描”的标记情况下，确定目标文件的目标文件指纹，以便进一步判定是否对目标文件进行病毒检测。

其中，第一预设条件可参照前文图 2 步骤 S202 中“预设条件”的相关表述，在此不再赘述。

作为一个示例，第一预设条件可以是目标文件元数据中存在“已扫描”的标记，如果目标文件元数据中存在“已扫描”的标记，代表目标文件已经进行过病毒检测并确认没有病毒，可以不对目标文件进行病毒检测；如果目标文件元数据中没有“已扫描”的标记，则在目标文件元数据中，读取目标文件指纹。

作为另一个示例，第一预设条件可以是目标文件元数据中记录的病毒检测次数达到预设检测次数，如果目标文件元数据中记录的病毒检测次数达到预设检测次数，可以不对目标文

件进行病毒检测；如果目标文件元数据中记录的病毒检测次数未达到预设检测次数，则可以在目标文件元数据中，读取目标文件指纹。

作为另一个示例，第一预设条件可以是目标文件元数据中记录的病毒检测时间与当前时刻的间隔未超过预设时间间隔，如果目标文件元数据中记录的病毒检测时间与当前时刻的间隔未超过预设时间间隔，可以不对目标文件进行病毒检测；如果目标文件元数据中记录病毒检测时间与当前时刻的间隔超过了预设时间间隔，则在目标文件元数据中，读取目标文件指纹。

作为另一个示例，第一预设条件可以是目标文件元数据中记录的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，如果目标文件元数据中记录的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，可以不对目标文件进行病毒检测；如果目标文件元数据中记录的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息不同，则在目标文件元数据中，读取目标文件指纹。

作为另一个示例，第一预设条件可以是目标文件元数据中存在“已扫描”的标记、目标文件元数据中记录的病毒检测时间与当前时刻的间隔未超过预设时间间隔、且目标文件元数据中记录的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，如果目标文件元数据中有“已扫描”的标记、记录的病毒检测时间与当前时刻的间隔未超过预设时间间隔、且执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，则可以不对目标文件进行病毒检测；否则，则在目标文件元数据中，读取目标文件指纹。

S703、根据目标文件指纹，在索引库中选取目标文件指纹对应的病毒检测的历史信息。

该步骤与上述图 6 中步骤 S602 相同，在此不再赘述。

S704、在目标文件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定对目标文件进行病毒检测。

其中，第二预设条件可参照前文图 2 中步骤 S202 中“预设条件”的相关表述，在此不再赘述。

在一种可能的实现方式中，在目标文件指纹对应的病毒检测的历史信息满足第二预设条件的情况下，确定不对目标文件进行病毒检测，并更新目标文件元数据中的病毒检测的历史信息。

示例性地，可以根据目标文件指纹对应的病毒检测的历史信息对目标文件元数据中的病毒检测的历史信息进行更新。例如，若目标文件的元数据中没有“已扫描”的标记，而目标文件指纹对应的病毒检测的历史信息中有“已扫描”的标记，则可以在目标文件的元数据中添加“已扫描”的标记。再例如，可以将目标文件的元数据中记录的病毒检测时间更新为目标文件指纹对应的病毒检测时间。目标文件指纹对应的病毒检测的历史信息满足第二预设条件表明目标文件指纹对应的文件内容经历过病毒检测且没有病毒，即目标文件的内容经历过病毒检测且没有病毒，则可以更新目标文件元数据中的病毒检测的历史信息，从而保证目标文件元数据中的病毒检测的历史信息为最新的病毒检测的历史信息，以便下一次触发病毒检测任务时通过目标文件元数据中的病毒检测的历史信息快速确定是否需要对目标文件进行病毒检测，或者是否需要获取目标文件指纹。

S705、在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求。

该步骤的具体实现过程可参照上述图 2 中步骤 S203 的相关表述，在此不再赘述。

在一种可能的实现方式中，在执行完上述步骤 S705 后，还可以获取目标防病毒系统反馈

的对目标文件进行病毒检测的结果；并根据病毒检测的结果，更新目标文件元数据中的病毒检测的历史信息，及索引库中与目标文件的文件指纹对应的病毒检测的历史信息。

这样，通过上述步骤 S701-S705，根据目标文件元数据中的病毒检测的历史信息和索引库中目标文件指纹对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经经历过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

作为一个示例，以病毒检测的历史信息包括是否经历过病毒检测为例。例如，可以读取目标文件元数据中是否有“已扫描”的标记，如果目标文件元数据中没有“已扫描”的标记，则确定目标文件的目标文件指纹，并在索引库中选取目标文件指纹对应的是否经历过病毒检测的信息；如果索引库中目标文件指纹对应的病毒检测的历史信息中没有“已扫描”的标记，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果索引库中目标文件指纹对应的病毒检测的历史信息中有“已扫描”的标记，代表目标文件的内容已经进行过病毒检测并确认没有病毒，则确定不对目标文件进行病毒检测；进一步地，可以在目标文件元数据中添加“已扫描”标记。

作为另一个示例，以病毒检测的历史信息包括病毒检测时间为例。可以在目标文件元数据中读取目标文件的内容所经历的病毒检测时间，如果元数据中记载的病毒检测时间与当前时刻的间隔超过了预设时间间隔，则确定目标文件指纹，并在索引库中选取目标文件指纹对应的病毒检测时间，如果目标文件指纹对应的病毒检测时间与当前时刻的间隔超过了预设时间间隔，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果目标文件指纹对应的病毒检测时间与当前时刻的间隔未超过预设时间间隔，则可以确定不对目标文件进行病毒检测；进一步地，可以根据目标文件指纹对应的病毒检测时间更新目标文件元数据中记载的病毒检测时间。

作为另一个示例，以病毒检测的历史信息包括执行病毒检测的防病毒系统的配置信息为例。可以在目标文件元数据中读取执行病毒检测的防病毒系统的配置信息，如果目标文件元数据中记载的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息不同，则确定目标文件指纹，并在索引库中选取目标文件指纹对应的执行病毒检测的防病毒系统的配置信息，如果目标文件指纹对应的病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息不同，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果目标文件指纹对应的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，则可以确定不对目标文件进行病毒检测；进一步地，可以根据目标文件指纹对应的执行病毒检测的防病毒系统的配置信息，更新目标文件元数据中记载的执行病毒检测的防病毒系统的配置信息。

作为另一个示例，以病毒检测的历史信息包括是否经历过病毒检测、病毒检测时间和执行病毒检测的防病毒系统的配置信息为例。可以在目标文件元数据中读取是否经历过病毒检测、病毒检测时间和执行病毒检测的防病毒系统的配置信息；如果目标文件元数据中有“已扫描”的标记、病毒检测的时间与当前时刻的间隔未超过预设时间间隔或执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同中任一项不满足，则确定目标文件指纹，并在索引库中选取目标文件指纹对应的是否经历过病毒检测的信息、病毒检测时间和执行病毒检测的防病毒系统的配置信息，如果目标文件指纹对应的病毒检测的信息中有“已扫描”的标记、对应的病毒检测的时间与当前时刻的间隔未超过预设时间间隔或对应的执行病

毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同中任一项不满足，则确定对目标文件进行病毒检测，并向目标防病毒系统发送对目标文件进行病毒检测的请求。如果目标文件指纹对应的病毒检测的信息中有“已扫描”的标记、对应的病毒检测的时间与当前时刻的间隔未超过预设时间间隔且对应的执行病毒检测的防病毒系统的配置信息与目标防病毒系统的配置信息相同，则可以确定不对目标文件进行病毒检测；进一步地，可以在目标文件的元数据中添加“已扫描”的标记，并根据目标文件指纹对应的的病毒检测的时间及对应的执行病毒检测的防病毒系统的配置信息更新目标文件元数据中病毒检测时间和执行病毒检测的防病毒系统的配置信息。

基于上述方法实施例的同一发明构思，本申请的实施例还提供了一种病毒检测装置，该病毒检测装置可以用于执行上述方法实施例所描述的技术方案。例如，可以执行上述图 2、图 5、图 6 或图 7 中所示方法的各步骤。

图 8 示出根据本申请一实施例的一种病毒检测装置的结构示意图。如图 8 所示，所述装置包括：获取模块 801，用于获取存储系统中目标文件对应的病毒检测的历史信息；其中，所述病毒检测的历史信息包括：是否经历过病毒检测、病毒检测次数、病毒检测时间、执行病毒检测的防病毒系统的配置信息中的至少一项；确定模块 802，用于根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测；请求模块 803，用于在确定对所述目标文件进行病毒检测的情况下，向目标防病毒系统发送对所述目标文件进行病毒检测的请求。

本申请实施例，目标文件对应的病毒检测的历史信息可以表征目标文件的内容所经历的病毒检测的相关信息；根据目标文件对应的病毒检测的历史信息确定是否对目标文件进行病毒检测，可以在保证数据安全的前提下，避免对已经进行过病毒检测的文件内容重复进行病毒检测，从而节约了网络带宽开销，节省了病毒检测时间，提升了病毒检测效率；此外，在触发在线病毒检测任务时，用户可以及时打开目标文件，提高了存储系统的读写性能。

在一种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括所述目标文件元数据中的病毒检测的历史信息，和/或，索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；其中，所述索引库中包括至少一个文件指纹及所述至少一个文件指纹对应的病毒检测的历史信息，所述至少一个文件指纹与所述存储系统中的一个或多个文件相关联，所述至少一个文件指纹对应的病毒检测的历史信息包括与所述至少一个文件指纹相关联的各文件对应的病毒检测的历史信息中最新的历史信息。

在一种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息；所述获取模块 801，还用于在所述目标文件元数据中，读取所述目标文件对应的病毒检测的历史信息。

在一种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述获取模块 801，还用于：确定所述目标文件的目标文件指纹；根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息。

在一种可能的实现方式中，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息，和，所述索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述确定模块 802，还用于：在所述目标文件元数据中的病毒检测的历史信息不满足第一预设条件的情况下，确定所述目标文件的目标文件指纹；根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息；在所述目标文

件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定对所述目标文件进行病毒检测。

在一种可能的实现方式中，所述装置还包括：结果反馈模块，用于获取所述目标防病毒系统反馈的对所述目标文件进行病毒检测的结果；更新模块，用于根据所述病毒检测的结果，更新所述目标文件对应的病毒检测的历史信息。

在一种可能的实现方式中，所述装置还包括：元数据更新模块，在所述目标文件指纹对应的病毒检测的历史信息满足第二预设条件的情况下，确定不对所述目标文件进行病毒检测，并更新所述目标文件元数据中的病毒检测的历史信息。

上述图 8 所示的病毒检测装置及其各种可能的实现方式的技术效果及具体描述可参见上述病毒检索方法的相关表述，此处不再赘述。

应理解以上病毒检测装置中各模块的划分仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。此外，装置中的模块可以以处理器调用软件的形式实现；例如装置包括处理器，处理器与存储器连接，存储器中存储有指令，处理器调用存储器中存储的指令，以实现以上任一种方法或实现该装置各模块的功能，其中处理器例如为通用处理器，例如中央处理单元（Central Processing Unit，CPU）或微处理器，存储器为装置内的存储器或装置外的存储器。或者，装置中的模块可以以硬件电路的形式实现，可以通过对硬件电路的设计实现部分或全部模块的功能，该硬件电路可以理解为一个或多个处理器；例如，在一种实现中，该硬件电路为专用集成电路（application-specific integrated circuit，ASIC），通过对电路内元件逻辑关系的设计，实现以上部分或全部模块的功能；再如，在另一种实现中，该硬件电路为可以通过可编程逻辑器件（programmable logic device，PLD）实现，以现场可编程门阵列（Field Programmable Gate Array，FPGA）为例，其可以包括大量逻辑门电路，通过配置文件来配置逻辑门电路之间的连接关系，从而实现以上部分或全部模块的功能。以上装置的所有模块可以全部通过处理器调用软件的形式实现，或全部通过硬件电路的形式实现，或部分通过处理器调用软件的形式实现，剩余部分通过硬件电路的形式实现。

在本申请实施例中，处理器是一种具有信号的处理能力的电路，在一种实现中，处理器可以是具有指令读取与运行能力的电路，例如 CPU、微处理器、图形处理器（graphics processing unit，GPU）、数字信号处理器（digital signal processor，DSP）、神经网络处理器（neural-network processing unit，NPU）、张量处理器（tensor processing unit，TPU）等；在另一种实现中，处理器可以通过硬件电路的逻辑关系实现一定功能，该硬件电路的逻辑关系是固定的或可以重构的，例如处理器为 ASIC 或 PLD 实现的硬件电路，例如 FPGA。在可重构的硬件电路中，处理器加载配置文档，实现硬件电路配置的过程，可以理解为处理器加载指令，以实现以上部分或全部模块的功能的过程。

可见，以上装置中的各模块可以是被配置成实施以上实施例方法的一个或多个处理器（或处理电路），例如：CPU、GPU、NPU、TPU、微处理器、DSP、ASIC、FPGA，或这些处理器形式中至少两种的组合。此外，以上装置中的各模块可以全部或部分可以集成在一起，或者可以独立实现，对此不作限定。

作为一个示例，病毒检测装置可以是独立设置，也可以集成在其他装置中，还可以是通过软件或者软件与硬件结合实现。例如，病毒检测装置可以为图 1 中的防病毒单元，可以集成在上述图 1 中存储系统 10 中。

作为另一个示例，病毒检测装置还可以为具有数据处理能力的设备或系统，或设置在这

些设备或系统中的部件或者芯片。例如，病毒检测装置可以是集成存储管理平台（Integrated Storage Management，DEVICE MANAGER）、云端服务器、台式机、便携式电脑、网络服务器、服务集群、掌上电脑（personal digital assistant，PDA）、移动手机、平板电脑、无线终端设备、嵌入式设备、医疗设备或其他具有数据处理功能的设备，或者为这些设备内的部件或者芯片。

本申请的实施例还提供了一种电子设备，包括：处理器；用于存储处理器可执行指令的存储器；其中，所述处理器被配置为执行所述指令时实现上述实施例的方法。示例性地，可以执行上述图 2、图 5、图 6 或图 7 中所示方法的各步骤。

图 9 示出根据本申请一实施例的一种电子设备的结构示意图，如图 9 所示，该电子设备可以包括：至少一个处理器 901，通信线路 902，存储器 903 以及至少一个通信接口 904。

处理器 901 可以是一个通用中央处理器，微处理器，特定应用集成电路，或一个或多个用于控制本申请方案程序执行的集成电路；处理器 901 也可以包括多个通用处理器的异构运算架构，例如，可以是 CPU、GPU、微处理器、DSP、ASIC、FPGA 中至少两种的组合；作为一个示例，处理器 901 可以是 CPU+GPU 或者 CPU +ASIC 或者 CPU+FPGA。

通信线路 902 可包括一通路，在上述组件之间传送信息。

通信接口 904，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如以太网，RAN，无线局域网（wireless local area networks，WLAN）等。

存储器 903 可以是只读存储器（read-only memory，ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory，RAM）或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器（electrically erasable programmable read-only memory，EEPROM）、只读光盘（compact disc read-only memory，CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过通信线路 902 与处理器相连接。存储器也可以和处理器集成在一起。本申请实施例提供的存储器通常可以具有非易失性。其中，存储器 903 用于存储执行本申请方案的计算机执行指令，并由处理器 901 来控制执行。处理器 901 用于执行存储器 903 中存储的计算机执行指令，从而实现本申请上述实施例中提供的方法；示例性地，可以执行上述图 2、图 5、图 6 或图 7 中所示方法的各步骤。

可选的，本申请实施例中的计算机执行指令也可以称之为应用程序代码，本申请实施例对此不作具体限定。

示例性地，处理器 901 可以包括一个或多个 CPU，例如，图 9 中的 CPU0；处理器 901 也可以包括一个 CPU，及 GPU、ASIC、FPGA 中任一个，例如，图 9 中的 CPU0+GPU0 或者 CPU 0+ASIC0 或者 CPU0+FPGA0。

示例性地，电子设备可以包括多个处理器，例如图 9 中的处理器 901 和处理器 907。这些处理器中的每一个可以是一个单核（single-CPU）处理器，也可以是一个多核（multi-CPU）处理器，或者是包括多个通用处理器的异构运算架构。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（例如计算机程序指令）的处理核。

在具体实现中，作为一种实施例，电子设备还可以包括输出设备 905 和输入设备 906。输出设备 905 和处理器 901 通信，可以以多种方式来显示信息。例如，输出设备 905 可以是液晶显示器（liquid crystal display，LCD），发光二级管（light emitting diode，LED）

显示设备，阴极射线管（cathode ray tube，CRT）显示设备，或投影仪（projector）等，例如，可以为车载 HUD、AR-HUD、显示器等显示设备。输入设备 906 和处理器 901 通信，可以以多种方式接收用户的输入。例如，输入设备 906 可以是鼠标、键盘、触摸屏设备或传感设备等。

本申请的实施例提供了一种计算机可读存储介质，其上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现上述实施例中的方法。示例性地，可以实现上述图 2、图 5、图 6 或图 7 中所示方法的各步骤。

本申请的实施例提供了一种计算机程序产品，例如，可以包括计算机可读代码，或者承载有计算机可读代码的非易失性计算机可读存储介质；当所述计算机程序产品在计算机上运行时，使得所述计算机执行上述实施例中的方法。示例性地，可以实现上述图 2、图 5、图 6 或图 7 中所示方法的各步骤。

计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是——但不限于——电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子（非穷举的列表）包括：便携式计算机盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、静态随机存取存储器（SRAM）、便携式压缩盘只读存储器（CD-ROM）、数字多功能盘（DVD）、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。这里所使用的计算机可读存储介质不被解释为瞬时信号本身，诸如无线电波或者其他自由传播的电磁波、通过波导或其他传输媒介传播的电磁波（例如，通过光纤电缆的光脉冲）、或者通过电线传输的电信号。

这里所描述的计算机可读程序指令可以从计算机可读存储介质下载到各个计算/处理设备，或者通过网络、例如因特网、局域网、广域网和/或无线网下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光纤传输、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或者网络接口从网络接收计算机可读程序指令，并转发该计算机可读程序指令，以供存储在各个计算/处理设备中的计算机可读存储介质中。

用于执行本申请操作的计算机程序指令可以是汇编指令、指令集架构（ISA）指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、或者以一种或多种编程语言的任意组合编写的源代码或目标代码，所述编程语言包括面向对象的编程语言—诸如 Smalltalk、C++等，以及常规的过程式编程语言—诸如“C”语言或类似的编程语言。计算机可读程序指令可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络—包括局域网(LAN)或广域网(WAN)—连接到用户计算机，或者，可以连接到外部计算机（例如利用因特网服务提供商来通过因特网连接）。在一些实施例中，通过利用计算机可读程序指令的状态信息来个性化定制电子电路，例如可编程逻辑电路、现场可编程门阵列（FPGA）或可编程逻辑阵列（PLA），该电子电路可以执行计算机可读程序指令，从而实现本申请的各个方面。

这里参照根据本申请实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本申请的各个方面。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机可读程序指令实现。

这些计算机可读程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理器，从而生产出一种机器，使得这些指令在通过计算机或其它可编程数据处理装置的处理器执行时，产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中，这些指令使得计算机、可编程数据处理装置和/或其他设备以特定方式工作，从而，存储有指令的计算机可读介质则包括一个制造品，其包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各个方面的指令。

也可以把计算机可读程序指令加载到计算机、其它可编程数据处理装置、或其它设备上，使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤，以产生计算机实现的过程，从而使得在计算机、其它可编程数据处理装置、或其它设备上执行的指令实现流程图和/或框图中的一个或多个方框中规定的功能/动作。

附图中的流程图和框图显示了根据本申请的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分，所述模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

以上已经描述了本申请的各实施例，上述说明是示例性的，并非穷尽性的，并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择，旨在最好地解释各实施例的原理、实际应用或对市场中的技术改进，或者使本技术领域的其它普通技术人员能理解本文披露的各实施例。

权 利 要 求 书

1. 一种病毒检测方法，其特征在于，所述方法包括：

获取存储系统中目标文件对应的病毒检测的历史信息；其中，所述病毒检测的历史信息包括：是否经历过病毒检测、病毒检测次数、病毒检测时间、执行病毒检测的防病毒系统的配置信息中的至少一项；

根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测；

在确定对所述目标文件进行病毒检测的情况下，向目标防病毒系统发送对所述目标文件进行病毒检测的请求。

2. 根据权利要求 1 所述的方法，其特征在于，所述目标文件对应的病毒检测的历史信息包括所述目标文件元数据中的病毒检测的历史信息，和/或，索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；其中，所述索引库中包括至少一个文件指纹及所述至少一个文件指纹对应的病毒检测的历史信息，所述至少一个文件指纹与所述存储系统中的一个或多个文件相关联，所述至少一个文件指纹对应的病毒检测的历史信息包括与所述至少一个文件指纹相关联的各文件对应的病毒检测的历史信息中最新的历史信息。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息；

所述获取目标文件对应的病毒检测的历史信息，包括：在所述目标文件元数据中，读取所述目标文件对应的病毒检测的历史信息。

4. 根据权利要求 1 或 2 所述的方法，其特征在于，所述目标文件对应的病毒检测的历史信息包括：索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；

所述获取目标文件对应的病毒检测的历史信息，包括：

确定所述目标文件的目标文件指纹；

根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息。

5. 根据权利要求 3 所述的方法，其特征在于，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息，和，所述索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；

所述根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测，包括：

在所述目标文件元数据中的病毒检测的历史信息不满足第一预设条件的情况下，确定所述目标文件的目标文件指纹；

根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息；

在所述目标文件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定对所述目标文件进行病毒检测。

6. 根据权利要求 1-5 中任一所述的方法，其特征在于，所述方法还包括：

获取所述目标防病毒系统反馈的对所述目标文件进行病毒检测的结果；

根据所述病毒检测的结果，更新所述目标文件对应的病毒检测的历史信息。

7. 根据权利要求 5 中所述的方法，其特征在于，所述方法还包括：

在所述目标文件指纹对应的病毒检测的历史信息满足第二预设条件的情况下，确定不对所述目标文件进行病毒检测，并更新所述目标文件元数据中的病毒检测的历史信息。

8. 一种病毒检测装置，其特征在于，所述装置包括：获取模块，用于获取存储系统中目标文件对应的病毒检测的历史信息；其中，所述病毒检测的历史信息包括：是否经历过病毒检测、病毒检测次数、病毒检测时间、执行病毒检测的防病毒系统的配置信息中的至少一项；确定模块，用于根据所述目标文件对应的病毒检测的历史信息，确定是否对所述目标文件进行病毒检测；请求模块，用于在确定对所述目标文件进行病毒检测的情况下，向目标防病毒系统发送对所述目标文件进行病毒检测的请求。

9. 根据权利要求 8 所述的装置，其特征在于，所述目标文件对应的病毒检测的历史信息包括所述目标文件元数据中的病毒检测的历史信息，和/或，索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；其中，所述索引库中包括至少一个文件指纹及所述至少一个文件指纹对应的病毒检测的历史信息，所述至少一个文件指纹与所述存储系统中的一个或多个文件相关联，所述至少一个文件指纹对应的病毒检测的历史信息包括与所述至少一个文件指纹相关联的各文件对应的病毒检测的历史信息中最新的历史信息。

10. 根据权利要求 8 或 9 所述的装置，其特征在于，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息；所述获取模块，还用于在所述目标文件元数据中，读取所述目标文件对应的病毒检测的历史信息。

11. 根据权利要求 8 或 9 所述的装置，其特征在于，所述目标文件对应的病毒检测的历史信息包括：索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述获取模块，还用于：确定所述目标文件的目标文件指纹；根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息。

12. 根据权利要求 10 所述的装置，其特征在于，所述目标文件对应的病毒检测的历史信息包括：所述目标文件元数据中的病毒检测的历史信息，和，所述索引库中与所述目标文件的文件指纹对应的病毒检测的历史信息；所述确定模块，还用于：在所述目标文件元数据中的病毒检测的历史信息不满足第一预设条件的情况下，确定所述目标文件的目标文件指纹；

根据所述目标文件指纹，在所述索引库中选取所述目标文件指纹对应的病毒检测的历史信息；在所述目标文件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定对所述目标文件进行病毒检测。

13. 根据权利要求 8-12 中任一所述的装置，其特征在于，所述装置还包括：结果反馈模块，用于获取所述目标防病毒系统反馈的对所述目标文件进行病毒检测的结果；更新模块，用于根据所述病毒检测的结果，更新所述目标文件对应的病毒检测的历史信息。

14. 根据权利要求 12 中所述的装置，其特征在于，所述装置还包括：元数据更新模块，在所述目标文件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定不对所述目标文件进行病毒检测，并更新所述目标文件元数据中的病毒检测的历史信息。

15. 一种电子设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行所述指令时实现权利要求 1-7 任意一项所述的方法。

16. 一种非易失性计算机可读存储介质，其上存储有计算机程序指令，其特征在于，所述计算机程序指令被处理器执行时实现权利要求 1-7 中任意一项所述的方法。

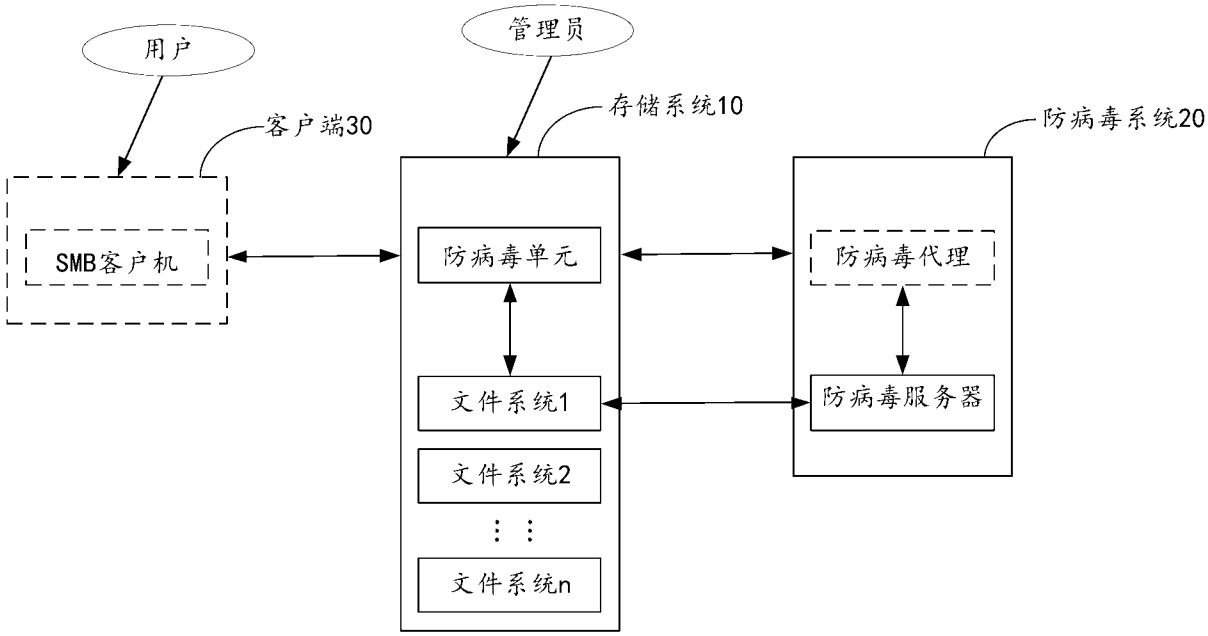
用户
管理员
客户端30
存储系统10
防病毒系统20
SMB客户机
防病毒单元
防病毒代理
文件系统1
防病毒服务器
文件系统2
文件系统n

图 1

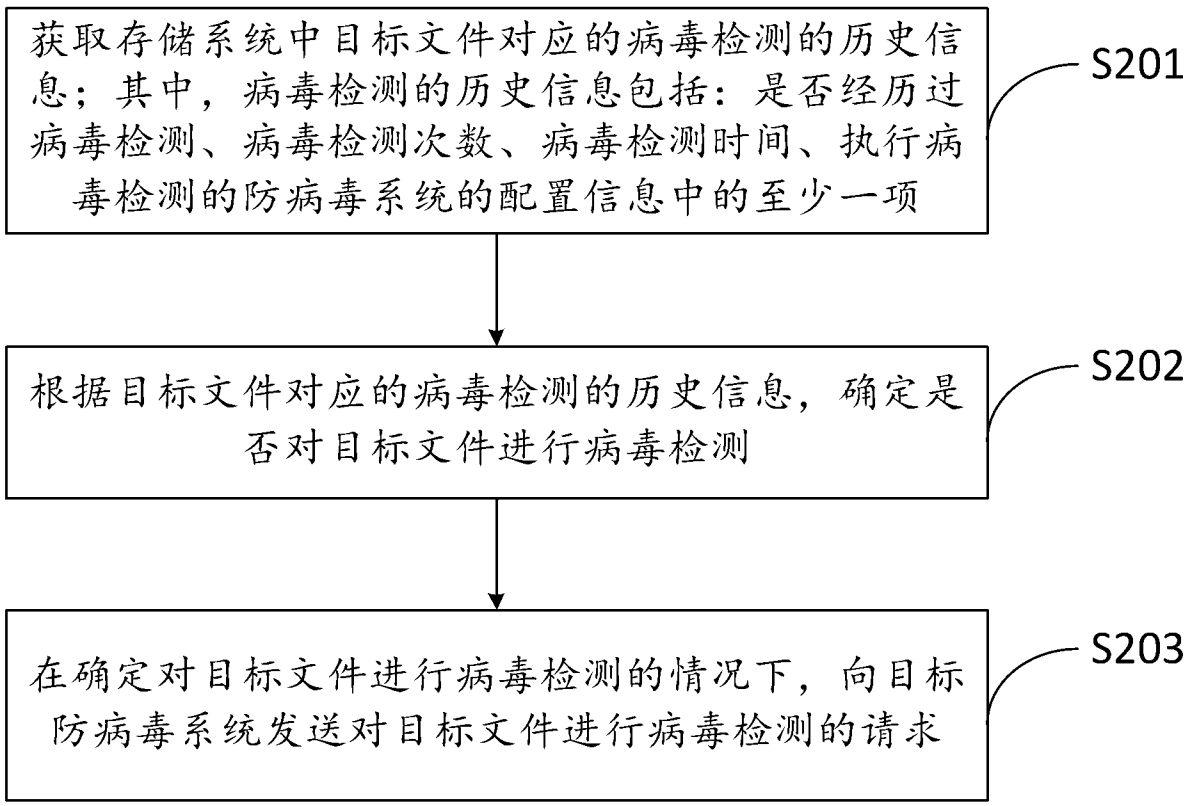
获取存储系统中目标文件对应的病毒检测的历史信息；其中，病毒检测的历史信息包括：是否经历过病毒检测、病毒检测次数、病毒检测时间、执行病毒检测的防病毒系统的配置信息中的至少一项
S201
根据目标文件对应的病毒检测的历史信息，确定是否对目标文件进行病毒检测
S202
在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求
S203

图 2

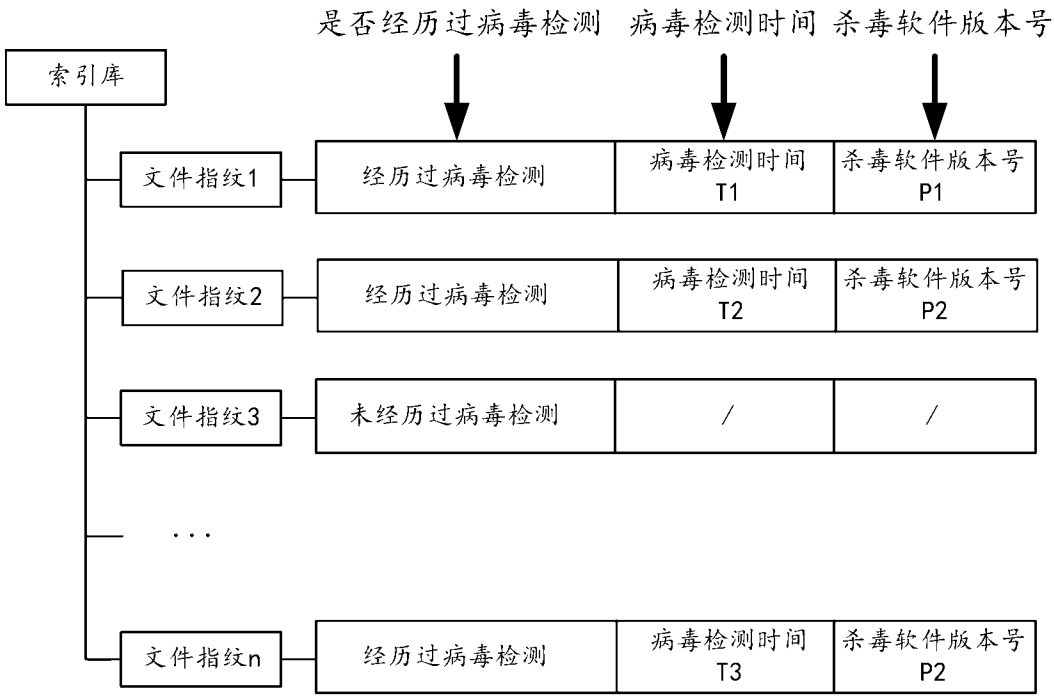

图 3

病毒检测的历史信息 / 文件	是否经历过病毒检测	病毒检测时间	杀毒软件版本号
文件A	是	2022年1月1日15时	p1
文件B	是	2022年1月1日13时	p2
文件C	否	\	\

↓

病毒检测的历史信息 / 文件指纹	是否经历过病毒检测	病毒检测时间	杀毒软件版本号
文件指纹1	是	2022年1月1日15时	p1

图 4

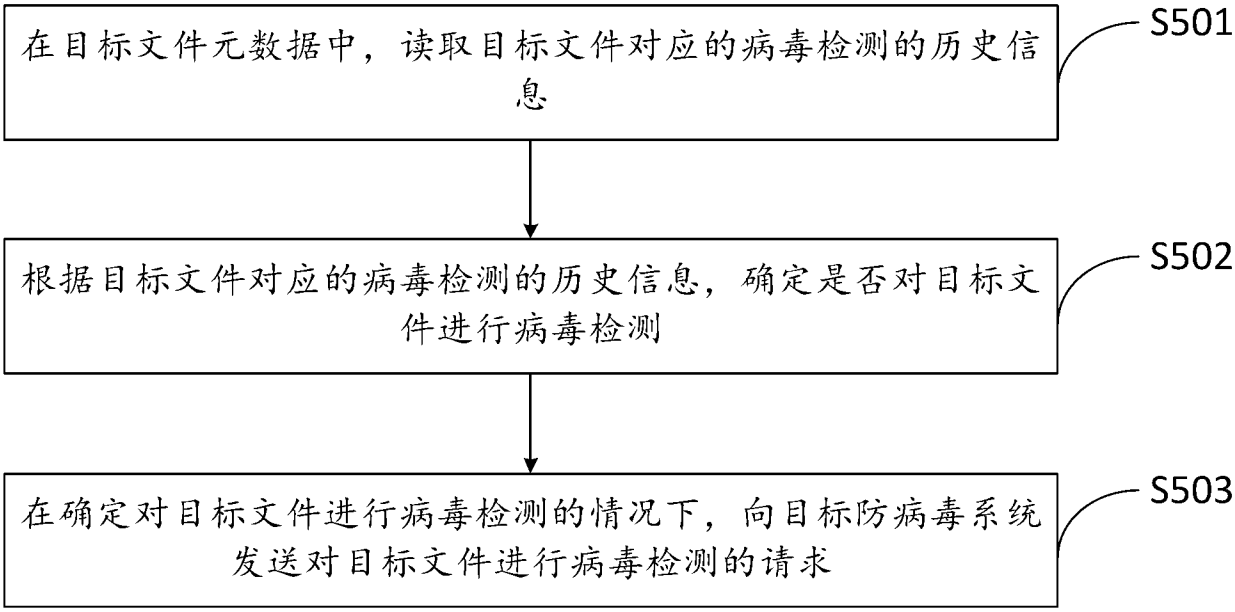
在目标文件元数据中，读取目标文件对应的病毒检测的历史信息
S501
根据目标文件对应的病毒检测的历史信息，确定是否对目标文件进行病毒检测
S502
在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求
S503

图 5

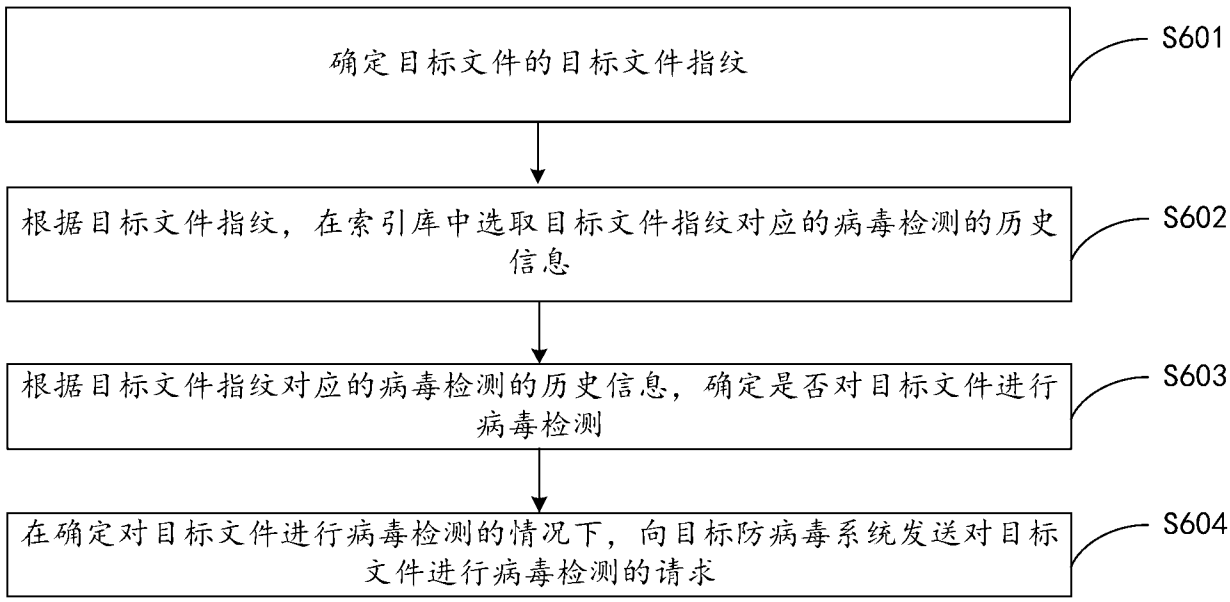
确定目标文件的目标文件指纹
S601
根据目标文件指纹，在索引库中选取目标文件指纹对应的病毒检测的历史信息
S602
根据目标文件指纹对应的病毒检测的历史信息，确定是否对目标文件进行病毒检测
S603
在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求
S604

图 6

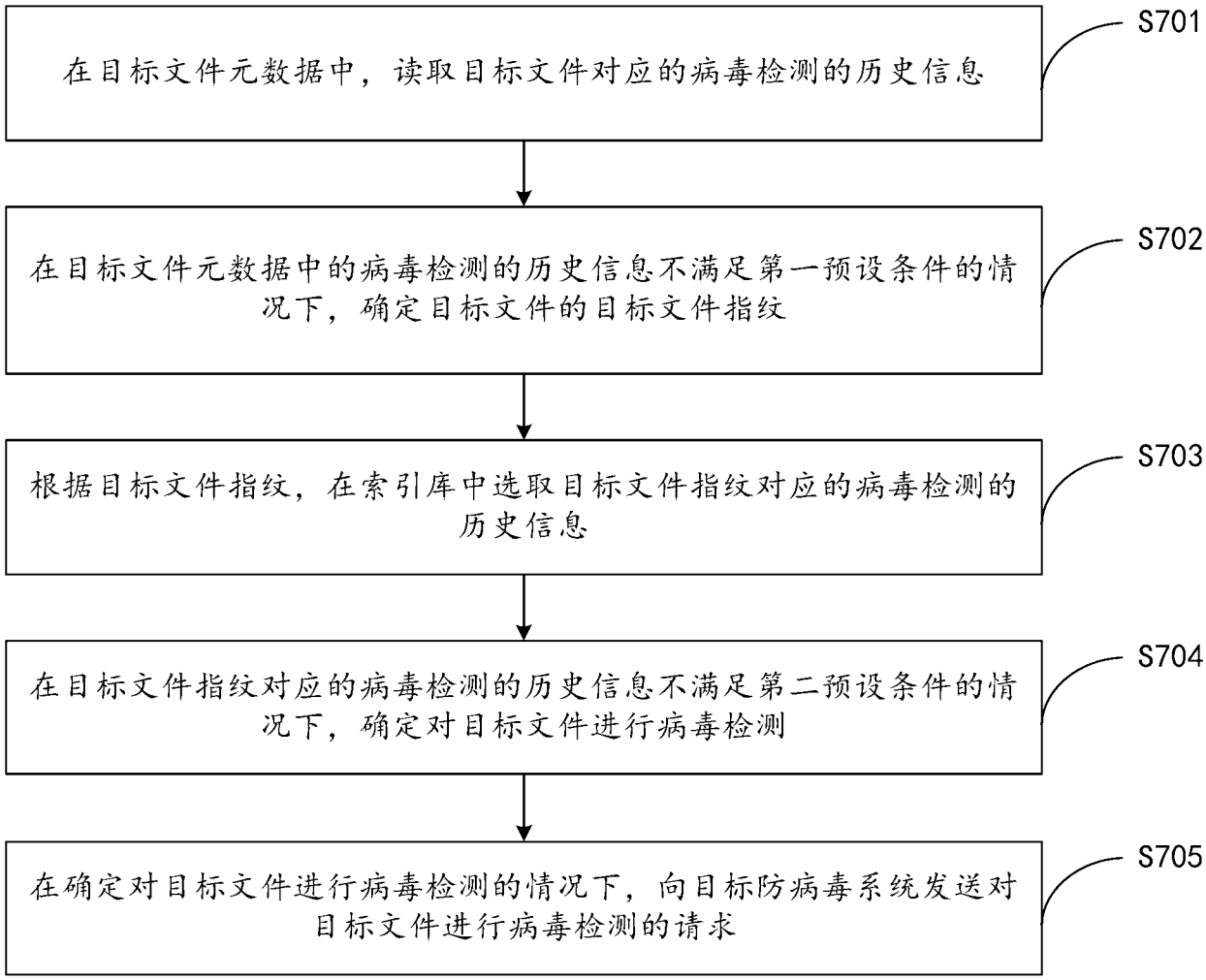
在目标文件元数据中，读取目标文件对应的病毒检测的历史信息
S701
在目标文件元数据中的病毒检测的历史信息不满足第一预设条件的情况下，确定目标文件的目标文件指纹
S702
根据目标文件指纹，在索引库中选取目标文件指纹对应的病毒检测的历史信息
S703
在目标文件指纹对应的病毒检测的历史信息不满足第二预设条件的情况下，确定对目标文件进行病毒检测
S704
在确定对目标文件进行病毒检测的情况下，向目标防病毒系统发送对目标文件进行病毒检测的请求
S705

图 7

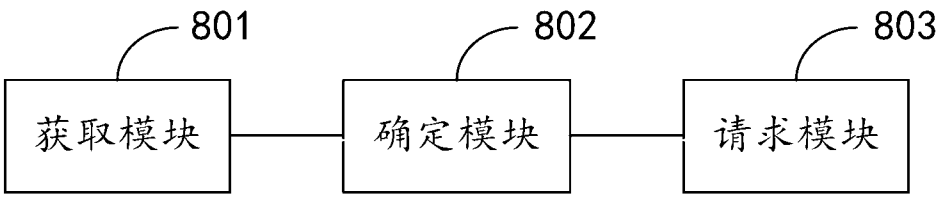
801
获取模块
802
确定模块
803
请求模块

图 8

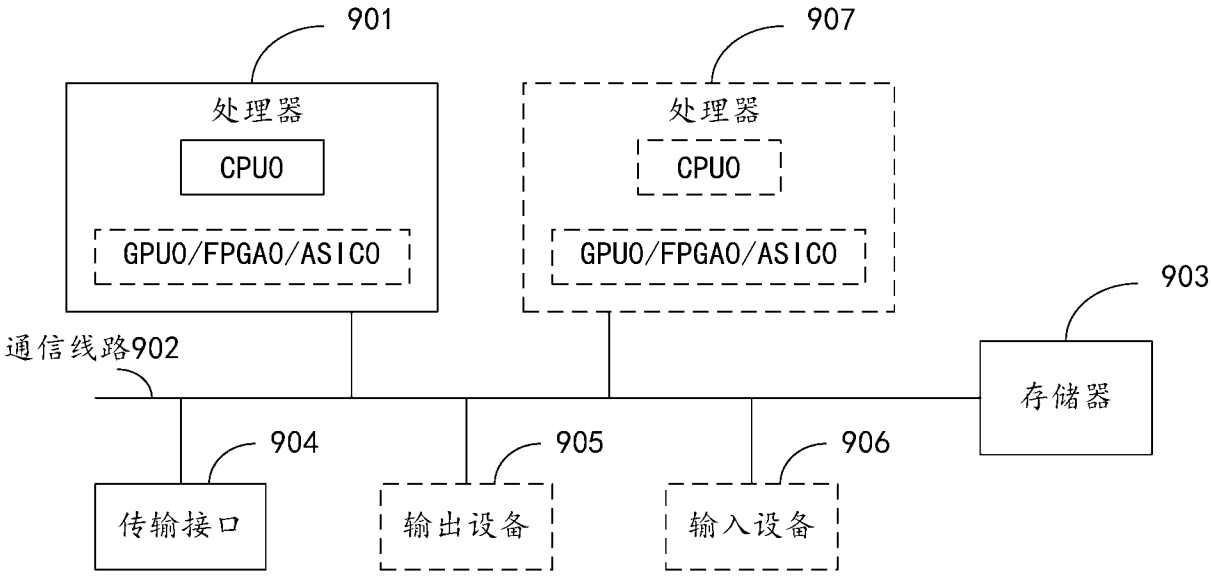
901
处理器
CPU0
GPU0/FPGA0/ASIC0
907
处理器
CPU0
GPU0/FPGA0/ASIC0
903
存储器
通信线路902
904
传输接口
905
输出设备
906
输入设备

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/087180

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)

IPC: 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)

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 病毒, 检测, 文件, 文档, 恶意, 木马, 历史, 记录, 信息, 次数, 时间, 版本, 请求, 发送, virus, detection, file, document, history, record, information, time, version, request, send

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103136474 A (YAO JIWEI et al.) 05 June 2013 (2013-06-05) description, paragraphs [0024]-[0048]	1-16
A	CN 113268765 A (HANGZHOU DBAPPSECURITY CO., LTD.) 17 August 2021 (2021-08-17) entire document	1-16
A	CN 102799823 A (BEIJING JIANGMIN XINKE TECHNOLOGY CO., LTD.) 28 November 2012 (2012-11-28) entire document	1-16
A	CN 108898014 A (ZHUHAI JUNTIAN ELECTRONIC TECHNOLOGY CO., LTD.) 27 November 2018 (2018-11-27) entire document	1-16
A	CN 110874473 A (CHENGDU HUAWEI TECHNOLOGIES CO., LTD.) 10 March 2020 (2020-03-10) entire document	1-16

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 June 2023	**13 June 2023**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/087180

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6763466 B1 (NETWORK ASSOCIATES TECHNOLOGY, INC.) 13 July 2004 (2004-07-13) entire document	1-16

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/087180

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 103136474 A	05 June 2013	None	
CN 113268765 A	17 August 2021	None	
CN 102799823 A	28 November 2012	None	
CN 108898014 A	27 November 2018	None	
CN 110874473 A	10 March 2020	None	
US 6763466 B1	13 July 2004	None	

国际检索报告

国际申请号
PCT/CN2023/087180

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)

IPC: 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））

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE：病毒，检测，文件，文档，恶意，木马，历史，记录，信息，次数，时间，版本，请求，发送，virus, detection, file, document, history, record, information, time, version, request, send

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
X	CN 103136474 A (姚纪卫 等) 2013年6月5日 (2013-06-05) 说明书第[0024]-[0048]段	1-16
A	CN 113268765 A (杭州安恒信息技术股份有限公司) 2021年8月17日 (2021-08-17) 全文	1-16
A	CN 102799823 A (北京江民新科技术有限公司) 2012年11月28日 (2012-11-28) 全文	1-16
A	CN 108898014 A (珠海市君天电子科技有限公司) 2018年11月27日 (2018-11-27) 全文	1-16
A	CN 110874473 A (成都华为技术有限公司) 2020年3月10日 (2020-03-10) 全文	1-16
A	US 6763466 B1 (NETWORKS ASSOCIATES TECHNOLOGY, INC.) 2004年7月13日 (2004-07-13) 全文	1-16

☐ 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

"D" 申请人在国际申请中引证的文件

"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	国际检索报告邮寄日期
2023年6月2日	2023年6月13日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 王璐 电话号码 (+86) 010-53961303

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/087180

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 103136474 A	2013年6月5日	无	
CN 113268765 A	2021年8月17日	无	
CN 102799823 A	2012年11月28日	无	
CN 108898014 A	2018年11月27日	无	
CN 110874473 A	2020年3月10日	无	
US 6763466 B1	2004年7月13日	无	