

数据安全保护方法、设备、系统、安全控制框架及存储介质

交叉引用

- 本申请引用于 2022 年 05 月 10 日递交的名称为“数据安全保护方法、装置、保护设备及存储介质”的第 202210504332.8 号中国专利申请，以及 2022 年 07 月 04 日递交的名称为“数据安全保护方法、装置、目标设备及存储介质”的第 202210781724.9 号中国专利申请，其通过引用被全部并入本申请。

技术领域

- 本申请涉及信息安全技术领域，尤其涉及一种数据安全保护方法、设备、系统、安全控制框架及存储介质。

背景技术

移动存储设备在日常工作生活中的应用十分广泛，但在使用移动存储设备接入计算机进行数据拷贝等数据处理操作时，容易产生数据风险问题。移动存储设备与计算机之间可能对彼此的数据安全产生威胁。

15 发明内容

本申请实施例提供了一种数据安全保护方法、设备、系统、安全控制框架及存储介质，可以保护存储设备与计算机设备的数据安全。

- 第一方面，本申请提供了一种数据安全保护方法，应用于目标设备，目标设备设有保护模块，保护模块包含至少一种保护模式，保护模式用于控制计算机设备在存储设备上的读写权限，方法包括：

根据目标设备的当前保护模式，对计算机设备发送的数据交互指令进行权限控制，数据交互指令用于计算机设备与存储设备进行数据交互；

若数据交互指令满足当前保护模式对应的权限要求，对数据交互指令做出响应。

- 25 具体的，所述数据安全保护方法，适用于保护模块，包括：

接收到计算机设备发送的数据交互指令时，确定当前保护模式，其中，

所述当前保护模式是所述保护模块预置的至少一种保护模式中的一个；

所述数据交互指令针对的数据源是所述当前保护模式指定的至少一个数据源中的一个，且所述数据交互指令对所述数据源内数据的操作类型符合所述当前保护模式规定的操作类型时，对所述数据交互指令做出响应；

- 5 其中，所述保护模块设置在所述计算机设备的用于连接存储设备的接口，或所述存储设备上，或中间设备上；

所述中间设备连接所述计算机设备与所述存储设备。

- 第二方面，本申请还提供一种数据安全保护模块，应用于目标设备，目标设备设有保护模块，保护模块包含至少一种保护模式，保护模式用于控制
10 计算机设备在存储设备上的读写权限，装置包括：

控制单元，用于根据目标设备的当前保护模式，对计算机设备发送的数据交互指令进行权限控制，数据交互指令用于计算机设备与存储设备进行数据交互；

- 响应单元，用于若数据交互指令满足当前保护模式对应的权限要求，对
15 数据交互指令做出响应。

第三方面，本申请还提供一种目标设备，设有保护模块和用于连接存储设备的第一接口，以及用于连接计算机的第二接口，所述保护模块包含至少一种保护模式，所述保护模式用于配置计算机设备在存储设备上的读写权限；

所述目标设备包括一个或多个处理器，以及存储器；

- 20 所述存储器用于存储计算机程序，所述计算机程序被所述处理器执行时实现如第一方面所述的数据安全保护方法的步骤。

第四方面，本申请还提供一种目标设备，设有集成于处理器的保护模块，所述保护模块包含至少一种保护模式，所述保护模式用于配置计算机设备在存储设备上的读取权限；

- 25 所述目标设备包括一个或多个处理器，以及存储器；

所述存储器用于存储计算机程序，所述计算机程序被所述处理器执行时实现如第一方面所述的数据安全保护方法的步骤。

第五方面，本申请还提供一种计算机可读存储介质，其存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面所述的数据安全保护方法的步骤。

第六方面，本申请还提供一种计算机程序产品，当计算机程序产品在计算机设备上运行时，使得计算机设备执行时实现第一方面的数据安全保护方法的步骤。

本申请还一实施例提供一种中间设备。该中间设备包括：

第一端口，用于连接计算机设备；

第二端口，用于连接存储设备；

10 交互模块，包括如下中的至少一种：触摸屏、语音交互装置、多个按键、滑动开关、具有至少两个选择的交互控件；以及

保护模块，连接在所述第一端口和所述第二端口之间，用于实现上述实施例提供的数据安全保护方法中的步骤。

本申请还一实施例提供一种设备系统，该系统包括：计算机设备，存储
15 设备以及上述实施例提供的中间设备。

本申请还一实施例提供一种存储设备，该存储设备包括：

第一端口，用于连接计算机设备；

保护芯片，用于实现上述实施例提供的所述数据安全保护方法中的步骤；

控制芯片，通过所述保护芯片与所述第一端口连接；

20 存储芯片，与所述控制芯片连接，用于在所述控制芯片的控制下，对存储空间内的数据进行存储管理。

本申请还一实施例提供一种存储设备，该存储设备包括：

第一端口，用于连接计算机设备；

25 控制芯片，其上部署有保护模块，用于实现上述实施例提供的所述数据安全保护方法中的步骤；

存储芯片，通过所述控制芯片与所述第一端口连接，用于在所述控制芯片的控制下，对存储空间内的数据进行存储管理。

本申请又一实施例提供了一种存储设备。该存储设备包括：

第一端口，用于连接计算机设备；

控制芯片，与第一端口连接，用于基于所述计算机设备发送的数据交互指令，生成相应的控制指令；

5 存储芯片，与所述控制芯片连接；

其中，所述存储芯片上部署有保护模块，用于采用上述实施例所述数据安全保护方法中的步骤，处理所述控制芯片发送的控制指令。

本申请还一实施例提供了一种安全控制框架。该安全控制框架包括：

配置模块，用于配置保护场景；

10 生成模块，用于生成保护场景的配置信息或带有所述保护场景的软件；

其中，一种保护场景对应至少一种保护模式；将所述配置信息或带有所述保护场景的软件部署在硬件设备上，使得所述硬件设备具有上述实施例所述数据安全保护方法中的步骤对应的功能。

与现有技术相比，本申请具备以下有益效果：

15 本申请通过在目标设备设置保护模块，以控制计算机设备在存储设备上的读写权限，从而保障存储设备之间的通信安全，避免恶意存储设备接入计算机设备而造成计算机数据安全风险，以及避免计算机设备恶意访问存储设备的隐私数据而造成存储设备的数据泄露。同时，本申请根据目标设备的当前保护模式，对计算机设备发送的数据交互指令进行权限控制，若数据交互
20 指令满足当前保护模式对应的权限要求，对数据交互指令做出响应，以保证计算机设备在目标设备的当前保护模式下访问存储设备，避免计算机设备上的病毒对存储设备造成数据破坏，也避免存储设备因被直接访问而造成数据泄露，从而提高存储设备的数据安全性。

25 附图说明

为了更清楚地说明本申请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申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其它的附图。

图 1 为本申请实施例示出的数据安全保护方法的流程示意图；

5 图 2a 为本申请实施例示出的目标设备的第一种结构形态对应的示意图；

图 2b 为本申请实施例示出的目标设备的第二种结构形态对应的示意图；

图 2c 为本申请实施例示出的目标设备的第三种结构形态对应的示意图；

图 3 为本申请第二实施例示出的数据安全保护方法的流程示意图；

图 4 为本申请实施例示出的步骤 S101 的具体流程示意图；

10 图 5 为本申请第三实施例示出的数据安全保护方法的流程示意图；

图 6a 示出了 U 盘无限制（可读可写）状态下的一个示例图；

图 6b~6d 示出了将外部 U 盘设置为全盘只读模式对应的示意图；

图 7 为本申请实施例示出的步骤 S102 的具体流程示意图；

15 图 8 为对比图，上部分为无保护模块的存储设备直接接入计算机设备在计算机设备上文件展示情况，下部分为具有保护模块的存储设备接入计算机设备后在计算机设备上文件展示情况；

图 9a 示出了在全局权限视角下可以看到根目录下文件的示意图；

图 9b 示出了在特定文件模式下映射至固定的特定文件夹只能看到特定文件的示意图；

20 图 9c 示出了在特定文件模式下继续新增一个文件的示意图；

图 9d 示出了在全局权限视角下可以看到根目录文件及新增文件的实施例；

图 10a~10d 示出了特定文件模式下空白文件为特定文件对应的示意图；

图 11a 和 11b 示出了全局权限视角下浏览 NEWFILE_1 文件和 NEWFILE_2 文件，这两个浏览的文件对应的目录；

25 图 12 为本申请第四实施例示出的数据安全保护方法的流程示意图；

图 13 为本申请第五实施例示出的数据安全保护方法的流程示意图；

图 14a、14c、14e 和 14g 示出了逻辑分盘模式对应的一个示例图；

图 14b 是从物理视角示出了对可用空间未进行逻辑分盘前的存储空间对应的示意图；

图 14d 是从物理视角示出了第 1 个分盘对应的 8GB 存储空间的示意图；

图 14f 是从物理视角示出了第 2 个分盘对应的 4GB 存储空间的示意图；

5 图 14h 是从物理视角示出了第 3 个分盘对应的 4GB 存储空间的示意图；

图 14i 示出了在保护模块未进行逻辑分盘时特定文件夹模式下响应计算机读写存储空间的示意图；

图 14j 示出了保护模块当前保护模式为逻辑分盘模式与特定文件夹模式的组合模式，并在逻辑分盘模式和特定文件夹模式的组合模式下选择逻辑分
10 盘 2 的示意图；

图 15 为本申请第六实施例示出的数据安全保护方法的流程示意图；

图 16 为本申请第七实施例示出的数据安全保护方法的流程示意图；

图 17 为本申请第八实施例示出的数据安全保护方法的流程示意图；

图 18a 示出了中间设备的一种结构形态实例；

15 图 18b 示出了集成有具有本申请各实施例提供的保护方法对应功能的保护模块的存储设备的示意图；

图 19 示出了 7 个具体场景的示意图；

图 20a 和 20b 示出了计算机设备与保护模块交互多个阶段的示意图；

图 21 示出了保护模块修改第一存储信息相关参数中的读写状态参数的示
20 意图；

图 22 示出了保护模块修改第一存储信息相关参数中的可格式化总块数和/或最后逻辑块地址的示意图；

图 23 示出了保护模块修改最后逻辑块地址对应的示意图；

图 24 示出了保护模块修改设备隐私信息对应的示意图；

25 图 25 示出了存储设备硬件初始化过程的示意图；

图 26a 示出了本申请各实施例提供的技术方案相关技术点的整理图；

图 26b 示出了采用本申请各实施例提供的技术方案带来的一些效果；

图 27 示出了分三种具体场景对响应计算机设备的读写交互指令的过程进行举例展示；

图 28a 示出了数据处理过程视角下控制“读指令(单扇区读)”、扇区地址、数据包或者状态的示意图；

5 图 28b 示出了数据处理过程视角下控制“读指令(多扇区连续读)”、扇区地址、数据包或者状态的示意图；

图 28c 示出了数据处理视角下控制“写指令(单扇区写)”、扇区地址、数据包或状态；

10 图 28d 示出了数据处理视角下控制“写指令(多扇区连续写)”、扇区地址、数据包或状态；

图 29 示出了计算机设备、保护模块及存储设备(如 U 盘、存储卡或存储芯片)的连接示意图；

图 30 为本申请实施例示出的数据安全保护模块的结构示意图；

图 31 为本申请实施例示出的目标设备的结构示意图。

15

具体实施方式

下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

20 如相关技术记载，当前存储设备与计算机设备之间可能对彼此的数据安全产生威胁。对于计算机设备：1.存储设备可能存在恶意代码，当计算机设备上的杀毒软件等安全软件无法查杀时，计算机设备会误拷贝并运行木马、病毒等恶意程序；2.存储设备可能存在恶意的硬件参数，在计算机读取时造成有
25 漏洞的安全软件的缓冲区溢出，从而执行预设的恶意指令；3.存储设备可能伪装成键盘和鼠标等输入设备，在接入计算机时执行预设的键盘或鼠标的输入

操作，向计算机拷贝并运行恶意程序或进行其他恶意输入操作。对于存储设备：1.计算机设备能够篡改或删除存储设备的数据，或者向存储设备写入木马或病毒等恶意程序；2.一些隐私文件数据能够被计算机设备读取和拷贝，甚至一些已经删除、隐藏的文件数据也有可能被计算机设备读取和拷贝，导致存储设备数据泄露。3、还有可能由于存储设备使用人保存不善，存储设备中的数据被窃取的问题。

在保护计算机设备方面，现有技术通常是在计算机中安装病毒查杀软件，对接入存储设备的文件进行扫描；或者安装存储设备接入控制软件，对没有预先登记的存储设备不予接入。不论是在计算机安装病毒查杀软件还是控制软件等，一是成本较高；对于计算机使用人来说，安装软件就需要占用一部分计算机资源，也需要花费软件费用；对于存储设备使用人来说，接入一个计算机时为了使用安全，需要接入的计算机上安装相应的软件，不太现实。二是，软件也是有局限性的，一些病毒木马等不能有效查杀。三是，安装软件的过程，也存在危险性。比如，软件来源出现问题，其中预先被捆绑了一些恶意程序，形成新的安全风险点。四是，软件需要对接入的设备的硬件特征参数进行判断，如果软件本身存在代码编写漏洞（例如存在缓冲区溢出等），恶意的设备可以通过发送恶意的硬件特征参数攻击软件，以恶意控制计算机设备。五是，现有的一些安全软件难以判断接入的设备是存储设备，还是鼠键设备，设备类型由接入设备自行上报（例如，外观为 U 盘的设备可以上报为大容量存储设备类型、或是鼠标设备类型、或是键盘设备类型，或是以上设备类型的集合），一些恶意设备向计算机设备上报鼠键类型，来恶意操作计算机设备。

现有技术主要偏向保护计算机设备，针对存储设备的保护方案较少。主要原因是：存储设备控制芯片的设计，一般无法对存储设备进行安全性功能的修改或安装安全软件。市面上有一种只读功能的存储设备，虽不能篡改存储设备中的数据，但数据还是可以被读取到的。还有一种具有数据加密功能的存储设备，该存储设备具备的加密功能，容易被逆向技术破解。

在介绍本申请各实施例之前，先对本文中的一些技术术语进行简单的说明。

USB 通信规则，USB 分为主机模式（计算机）和从机模式（U 盘）。主机主动向从机发送数据交互指令，从机根据数据交互指令进行被动响应。

5 关于枚举的原理，对 U 盘等存储设备来说，枚举就是计算机读取存储设备的过程。对于移动存储设备（大容量存储设备），一是读取硬件基本参数，包括硬件描述符、配置描述符、端口描述符、端点描述符的参数，并按照不同的参数加载驱动信息，实现硬件能够连接。二是读取移动存储设备参数，例如容量大小、是否为只读等等；三是读取文件系统信息，使之能够在计
10 算机操作系统上显示盘符。但是，在保护模块使用过程中，不一定严格遵守操作系统的枚举过程，但是一定是读取了移动存储设备枚举所必要的数据。

文件、文件夹的区别：根据部分的文件系统协议（例如 FAT32、ExFAT 等文件系统），上述提及的根目录与特定文件夹本质上是一样的，根目录为特殊的文件夹。文件夹与文件本质上是一样的，文件夹只是一种特殊的文件。

15 例如，文件名为 A.txt 的文件，存储的内容可以为“123456”；名为 showdir 的文件夹，存储的内容是其目录下的文件夹或文件信息。例如，test.txt 文件的属性和数据的首扇区地址，或者 test2 文件夹的属性和首扇区地址。当进一步读取 test.txt 文件的首扇区地址数据时，能读取到文件内容为“123456”。

字节位	0-7	8-10	11	12	13-15	16-17	18-19	20-21	22-23	24-25	26-27	28-31
参数	文件名	扩展名	保留	文件属性	创建时间	创建日期	最后访问日期	开始簇高字节	最后修改时间	最后修改日期	开始簇低字节	文件大小
示例数据 0x	41 20 20 20 20 20 20 20	54 58 54	20	10	a4 0a b4	a8 56	a8 56	00 00	c8 b3	a8 56	1d 00	06 00 00 00

（表 1）

20 表 1 以 FAT32 文件系统为例（A.txt 文件信息）：起始簇号为 0x1d，根据文件系统的计算，可得到首扇区（开始扇区地址）；在 FAT 表中可得到对应的簇链，并根据簇链进行计算，可得到文件数据的扇区地址集合。扇区地址集合的数据为 A.txt 文件的内容数据，例如 123456 字符串的二进制数据。

字节位	0-7	8-10	11	12	13-15	16-17	18-19	20-21	22-23	24-25	26-27	28-31
参数	文件名	扩展名	保留	文件属性	创建时间	创建日期	最后访问日期	开始簇高字节	最后修改时间	最后修改日期	开始簇低字节	文件大小
示例数据 0x	53 48 4f 57 44 49 52 20	20 20 20	10	08	53 91 b1	a8 56	a8 56	00 00	92 b1	a8 56	09 00	00 00 00 00

(表 2)

5 表 2 以 FAT32 文件系统为例 (showdir 文件夹) : showdir 文件夹起始簇号为 0x09, 根据本测试存储设备的文件系统计算, 得到对应的首扇区 (开始扇区地址) 为: 0x00010038 (注: 不同的文件系统、存储设备计算得到的扇区地址不同)。在 FAT 表中可得到对应的簇链, 并根据簇链进行计算, 可得到文件数据的扇区地址集合。扇区地址集合的数据为 showdir 文件夹包含的子
10 文件夹和文件信息, 例如 A.txt 文件的信息或者与 showdir 文件夹数据结构一致
的子文件夹信息。

本申请第一个实施例提供的一种保护模块, 该保护模块可以是一个独立设备 (又可称为中间设备), 用于连接存储设备与计算机设备。例如, 便携式
15 设备, 还可以是固定在计算机设备上的 USB 防护接口。它可称为: 便携式 U 盘硬件防火墙, 移动存储介质数据摆渡设备 (人工确认模式), 安全 USBHUB 等。其中, 移动存储介质可包括: U 盘、TF 卡、SD 卡、移动硬盘等等。该保护模块还可以是具有本申请各实施例提供的保护方法对应功能的存储设备, 该存储设备可以称为: 新型的安全 U 盘或移动硬盘、可以分盘的 U 盘或是对
20 应的存储卡 (如 TF 卡、SD 卡等)。该存储设备还可以为: 中间保护 (USB 接口)、读卡器 (SD、TF 卡接口) 和存储芯片同时存在的设备, 可通过滑动开关、触摸屏、按键、至少两个选择的交互控件等选择接入的物理数据源。该存储设备还可以是联网存储盘形态, 可以切换不同的网络数据源。本申请

各实施例提供的技术方案中，在软件形态上做了创新，如保护模块可具有至少一种保护模式，例如，只读模式、特定文件模式、空白文件模式、逻辑分盘模式、扇区限位模式、文件类型限制模式、加密写入模式、解密读出模式、人工确认模式、硬件类型接入保护模式、存储设备的数据信息保护模式、设备隐私保护模式、备份模式等中的至少一个。

该保护模块可以小体积，使用者能够随身携带或者长期固定在计算机设备的数据接口（USB 接口）上或固定在存储设备的接口上。该保护模块可为计算机设备与存储设备之间物理通信传输的中间设备，并按照使用人的设置对通信传输数据包进行安全限制或安全修改等控制，保护计算机或接入的存储设备；还可以在存储设备中集成采用本申请实施例提供的技术方案对应的保护模块，无需上述中间设备。集成有保护模块或安全主控芯片的存储设备，可按照用户的设置，保护存储设备的数据安全。

本申请实施例提供的技术方案，存储设备与计算机设备的通信数据收发经过中间设备控制后再进行传输，将计算机设备与存储设备之间隔离开，互相不能直接从对方处获取数据。其中，中间设备可以采用无操作系统的固件形式，带有恶意程序的计算机设备或存储设备难以通过漏洞修改中间设备的工作逻辑。中间设备可以采用标准通信协议，能够匹配操作系统自带的大容量存储设备驱动运行，接入计算机设备时可以无需安装驱动程序，同时能够连通大部分存储设备。

中间设备使用人可通过操作中间设备上的按钮或开关等可选择的交互控件的方式，按照向移动存储设备写入数据或读出数据等的不同使用场景，进行存储设备的只读模式、特定文件模式、空白文件模式、逻辑分盘模式、扇区限位模式、文件类型限制模式、加密写入模式、解密读出模式、人工确认模式、硬件类型接入保护模式、存储设备的数据信息保护模式、设备隐私保护模式、备份模式等保护模式的设置。同时，中间设备还带有文件内容数据加密、日志留存和扩展设置等三种辅助设置。

即本申请提供一种数据安全保护方法，通过在目标设备设置保护模块，

以配置计算机设备在存储设备上的读写权限，从而保障存储设备之间的通信安全，避免恶意存储设备接入计算机设备而造成计算机数据安全风险，以及避免计算机设备恶意访问存储设备的隐私数据而造成存储设备的数据泄露，并且可以无需计算机设备安装安全软件，有效规避安装安全软件所存在的安全风险。同时，本申请根据目标设备的当前保护模式，对计算机设备发送的数据交互指令进行权限控制，若数据交互指令满足当前保护模式对应的权限要求，对数据交互指令做出响应，以保证计算机设备在目标设备的当前保护模式下访问存储设备，避免计算机设备上的病毒对存储设备造成数据破坏，也避免存储设备因被直接访问而造成数据泄露，以及保护模块设于目标设备，能够有效规避恶意程序从计算机操作系统层面破解保护模块的保护模式，进一步提高存储设备的数据安全性。

请参照图 1，图 1 为本申请实施例提供的一种数据安全保护方法的流程示意图。本申请实施例的数据安全保护方法可应用于目标设备，所述目标设备设有保护模块，所述保护模块包含至少一种保护模式，所述保护模式用于控制计算机设备在存储设备上的读写权限。

可选地，目标设备为具有保护模块的中间设备，以作为存储设备与计算机设备建立通信连接时的中间连接节点。可以理解的是，通信连接包括有线连接和无线连接。示例性地，在一种有线连接场景下，如图 2a 示出的一种中间设备的结构示意图，中间设备 200 设有第一接口 201 和第二接口 202，第一接口 201 用于连接存储设备，第二接口 202 用于连接计算机设备。在将存储设备与计算机设备需要建立通信连接时，将存储设备与中间设备的第一接口 201 连接，并将中间设备 200 的第二接口 202 与计算机设备连接。需要说明的是，第一接口的数量可以为多个，以使中间设备能够同时接入多个存储设备；第一接口和第二接口可以为通用串行总线（Universal Serial Bus, USB）接口。第一接口还可以包括 eMMC (Embedded Multi Media Card) 接口，以直接接入 SD 卡和 TF 卡等，以及可以包括 SATA (Serial Advanced Technology Attachment) 接口、NVMe (NVM Express)、M.2 等数据接口，以直接接入硬盘、闪存、

SSD 存储设备等。应理解，图 2a 所示中间设备的结构仅用作示例而非限定，在其他实施例中可以包含更多或更少的部件，如图 2b 所示的结构等等，在此不再赘述。图 2b 中第一接口 201 可以为插槽形接口。图 2c 示出了集成有保护模块的存储设备的一种结构形态示例图。用户可通过交互控件（比如操作
5 存储设备上的控件）选择保护模块的当前保护模式。

可选地，目标设备为具有保护模块的存储设备，保护模块可集成于存储设备的芯片（处理器）、集成电路或硬件内部中，以使存储设备具备本申请实施例的数据安全保护方法的功能。可以理解的是，对于目标设备为中间设备时，由中间设备将计算机设备（或存储设备）发送的数据转发至存储设备
10 （或计算机设备），对于目标设备为具有保护模块的存储设备时，则由计算机设备（或存储设备）直接向存储设备（或计算机设备）发送数据，但需要由存储设备中的保护模块对接收到（或待发送）的数据进行权限控制等处理。对此，后续不再赘述。需要说明的是，当目标设备为具有保护模块的中间设备时，存储设备可以为不具有保护模块的存储设备。

15 可选地，存储设备包括但不限于 U 盘（USB 闪存盘）、移动硬盘、硬盘、读卡器（SD 卡、TF 卡）、外置光驱等，存储设备还可以具备联网功能；计算机设备包括但不限于笔记本电脑、桌上型计算机、嵌入式设备、物联网设备和工业控制设备等。

可选的，所述保护模块还可设置在所述计算机设备的用于连接存储设备的接口处。
20

本申请另一实施例提供一种连接在计算机和移动存储设备之间的中间设备（或模块），解决移动存储设备（例如，U 盘、SD 卡、移动光驱、移动硬盘等），在接入计算机进行拷贝数据时，由于目前通信协议和相关技术没有对数据权限进行限制，从而产生数据风险的问题。

25 可见，本申请实施例提供的方案存在两种交互逻辑：一是作为中间设备的交互逻辑：计算机设备发送指令->中间设备权限控制->存储设备响应->读写内部存储介质。

另一种是作为集成设备（例如具有保护模块的存储设备），交互逻辑缩减为：计算机设备发送指令—>存储设备的控制芯片筛选和响应（硬件集成：保护芯片+控制芯片；软件集成：控制芯片具有保护方法模块+控制读写模块）—>读写内部存储介质。

5

如图 1 所示，本申请实施例的数据安全保护方法包括步骤 S101 至步骤 S102，详述如下：

步骤 S101，根据所述目标设备的当前保护模式，对所述计算机设备发送的数据交互指令进行权限控制，所述数据交互指令用于所述计算机设备与
10 所述存储设备进行数据交互。

即上述步骤 S101 之前可包括：接收到计算机设备发送的数据交互指令时，确定当前保护模式，其中，所述当前保护模式是所述保护模块预置的至少一种保护模式中的一个。

其中，“对所述数据交互指令进行权限控制”可具体为：

15 判断所述数据交互指令针对的数据源是否是所述当前保护模式指定的至少一个数据源中的一个；

判断所述数据交互指令对所述数据源内数据的操作类型是否符合所述当前保护模式规定的操作类型。

20 所述数据交互指令针对的数据源是当前保护模式指定的至少一个数据源中的一个，且所述数据交互指令对所述数据源内数据的操作类型符合当前保护模式规定的操作类型时，所述数据交互指令满足当前保护模式对应的权限要求。

在具体实施时，若所述保护模块为中间设备或存储设备，该中间设备或存储设备上带有交互装置时，本实施例提供的所述方法还可包括如下步骤：

25 A、响应于用户在所述第一设备的交互装置上的操作，获取用户在所述至少一个保护模式中选出的目标保护模式；

B、将所述目标保护模式作为所述保护模块的当前保护模式；

其中，所述交互装置包括如下中的至少一种：触摸屏、语音交互装置、多个按键、滑动开关、具有至少两个选择的交互控件。

其中，上述具有至少两个选择的交互控件，如旋钮开关、具有多个停止档位的开关、具有多个拨动姿态的开关等等。

- 5 可选地，中间设备或具有所述保护模块的存储设备上也可没有交互装置。当前保护模式可以预先设置，也可以实时设置。具体地，其可以通过拨动开关、远程遥控、计算机配置的方式进行设置。示例性地，在一种可能实施的方式中，目标设备（如上文中提及的中间设备或具有保护模块的存储设备）设置有用以选中保护模式的物理开关，通过拨动物理开关以选中当前保护模
- 10 式。在另一种可能实施的方式中，目标设备设置有如蓝牙、红外线或超宽带的通信单元，以用于与远程遥控设备进行连接，从而通过远程遥控设备选中当前保护模式。在又一种可能实施的方式中，目标设备与具有全局权限的计算机设备通信连接，通过该计算机设备选中当前保护模式。需要说明的是，对于计算机配置方式，其应当在存储设备与计算机设备进行数据交互前进行
- 15 设置。

- 在本步骤中，保护模式包括但不限于全盘只读模式、特定文件读写模式、限位读写模式、文件限制读写模式、解密读取模式、加密写入模式和逻辑分盘模式。全盘只读模式表示允许读取存储设备中的所有文件，特定文件读写模式表示允许读写存储设备中的特定文件，限位读写模式表示允许读写存储
- 20 设备中目标扇区地址对应的文件，文件限制读写模式表示允许读写存储设备中具有目标文件特征的文件，解密读取模式表示对读取过程的数据进行解密，加密写入模式表示对写入过程的数据进行加密，逻辑分盘模式表示对存储设备进行分盘并接入到计算机的模式。

- 更具体的，所述至少一个保护模式可包括但不限于：只读模式、特定文
- 25 件模式、空白文件模式、扇区限位模式、文件类型限制模式、加密写入模式、解密读出模式、人工确认模式、逻辑分盘模式、硬件类型接入保护模式、存储设备的数据信息保护模式、设备隐私保护模式、备份模式等等。其中，

只读模式，所述只读模式指定的数据源为存储设备的全盘数据，规定的操作类型为只读类型；上文中的全盘只读模式可以理解为只读模式。

特定文件模式，所述特定文件模式指定的数据源为存储设备中的至少一个特定文件，规定的操作类型为读类型、或写类型、或读写类型。

- 5 空白文件模式，所述空白文件模式指定的数据源为存储设备中自动创建和/或人工创建的至少一个空白文件，规定的操作类型为写类型或读写类型。

扇区限位模式，所述扇区限位模式指定的数据源为存储设备中的至少一个特定扇区区间，规定的操作类型为读类型、或写类型、或读写类型。

- 10 文件类型限制模式，文件类型限制模式指定的数据源为存储设备中的至少一种特定类型的文件，规定的操作类型为读类型，或写类型、或读写类型。

加密写入模式，所述加密写入模式指定的数据源为存储设备中的至少一个第一扇区区间内的数据、至少一个第一文件和/或至少一种类型的文件，规定的操作类型为写类型。

- 15 解密读出模式，所述解密读出模式指定的数据源为存储设备中的至少一个第二扇区区间内的数据、至少一个第二文件和/或至少一种类型的文件，规定的操作类型为读类型。

人工确认模式，所述人工确认模式指定的数据源为存储设备中的至少一个第三扇区区间内的数据、至少一个第三文件和/或至少一种类型的文件，规定的操作类型为读写类型。

- 20 逻辑分盘模式，所述逻辑分盘模式指定的数据源为存储设备中的至少一个分盘，规定的操作类型为读类型，或写类型，或读写类型。

硬件类型接入保护模式，所述硬件类型接入保护模式无指定数据源，在所述硬件类型接入保护模式下判定存储设备是否为指定的设备类型；

- 25 存储设备的数据信息保护模式，所述存储设备的数据信息保护模式无指定数据源，在所述存储设备的数据信息保护模式下，对向计算机设备发送的存储设备的数据信息进行保护性处理，在枚举阶段将保护性处理后的存储设备的数据信息发送至所述计算机设备。

设备隐私保护模式，所述设备隐私保护模式无指定数据源，在所述设备隐私保护模式下，对向计算机设备发送的设备隐私信息进行保护性处理。

其中，保护性处理可包括但不限于：对存储设备的硬件特征参数进行保护性处理（如包装、删减等）、对存储设备的存储信息相关参数进行保护性处理、对存储设备的设备信息（如厂商信息等）进行保护性处理以保护存储设备的设备隐私等等。

备份模式，所述备份模式无指定数据源，在备份模式下，对计算机设备写入的数据同步写入至指定的备份存储区域内，和/或保护模块在执行写入指令之前读取所述计算机设备写入的扇区地址数据并写入至指定的备份存储区域内，和/或将接入的存储设备的重要数据扇区的数据备份存储至指定的备份存储区域内；若触发还原，则将所述指定的备份存储区域内的数据读出，写入至所述存储设备原有的数据扇区内。

上述各保护模式也可以多种模式组合。例如，逻辑分盘模式、特定文件模式、扇区限位模式，这三种模式可组合，这样当前保护模式为这三种模式组合后的组合模式。在该组合模式下，可以逻辑分盘后，限定操作特定文件，并通过扇区限位，对特定文件之外的文件不可进行读写。

这里需要补充的是：本实施例中的权限控制为基于当前保护模式对应的读写范围，对计算机设备与存储设备之间的数据交互进行控制的过程。其应理解为广义上的权限控制，即只要能达到对数据交互进行控制的目的，则属于本申请实施例定义的权限控制。

可选地，读写权限包括只读权限、只写权限和可读可写权限。在不同保护模式下，读写权限可以是针对不同对象的只读权限、只写权限或可读可写权限。例如，对于全盘只读模式，其读写权限为针对存储设备的所有文件的只读权限；对于特定文件读写模式，其读写权限为针对特定文件的只读权限、只写权限和可读可写权限中的至少一种。可以理解的是，其他模式的读写权限可以基于上述举例思想得出，在此不再赘述。

步骤 S102，若所述数据交互指令满足所述当前保护模式对应的权限要求，

对所述数据交互指令做出响应。

具体的，所述数据交互指令针对的数据源是所述当前保护模式指定的至少一个数据源中的一个，且所述数据交互指令对所述数据源内数据的操作类型符合所述当前保护模式规定的操作类型时，对所述数据交互指令做出响应。

5 在本步骤中，数据交互指令包括计算机设备发送的用于读取存储设备中的数据的数据读取指令，和用于向存储设备中写入数据的数据写入指令。可以理解的是，当读写权限为读取权限时，可支持数据读取指令；当读写权限为写入权限时，可支持数据写入指令；当读写权限为可读可写权限时，可支持数据读取指令和数据写入指令。

10 在一种可能实施的方式中，若目标设备为具有保护模块的中间设备，中间设备接收计算机设备发送的数据交互指令，并基于当前保护模式对该数据交互指令进行权限控制，若数据交互指令符合权限要求，则将该数据交互指令转发至存储设备，以使存储设备执行该数据交互指令对应的读写操作。在另一种可能实施的方式中，若目标设备为具有保护模块的存储设备，该存储
15 设备接收计算机设备发送的数据交互指令，并通过保护模块的当前保护模式对该数据交互指令进行权限控制，若数据交互指令符合权限要求，则存储设备执行该数据交互指令对应的读写操作。

需要说明的是，本申请通过多种保护模式对计算机设备和存储设备进行保护，能够满足用户在不同保护场景的应用需求；同时通过目标设备的保护
20 模型进行权限控制，提高计算机设备和存储设备的安全性。

在一些实施例，在图 1 所示实施例的基础上，图 3 示出了第二实施例的数据安全保护方法的流程示意图。与图 1 相同的步骤在此不再赘述。图 3 所示，所述方法还包括：

步骤 S301,若检测到所述计算机设备与所述存储设备之间的通信连接请
25 求，则识别所述第一接口的设备类型；

步骤 S302，若所述设备类型为预设允许通信类型，则建立所述计算机设备与所述存储设备之间的通信连接。

在本实施例中，预设允许通信类型包括但不限于大容量存储设备类型或其他预设的安全类型。可选地，第一接口的设备类型可以通过读取到的描述符参数进行确定。可以理解的是，对于目标设备为具有保护模块的中间设备，通过中间设备的第一接口向存储设备读取存储设备的描述符参数。对于目标
5 设备为具有保护模块的存储设备，则该存储设备可以调取其预先存储的描述符参数。

在一些实施例中，若所述目标设备为具有保护模块的中间设备，所述中间设备设有用于连接存储设备的第一接口，和用于连接计算机设备的第二接口；所述步骤 S301 之前，还包括：

10 当所述第一接口接入所述存储设备，且所述第二接口接入所述计算机设备时，检测所述计算机设备与所述存储设备之间的通信连接请求。

在本实施例中，当中间设备分别接入存储设备和计算机设备时，中间设备上电，中间设备在对存储设备的数据信息进行分析后判定符合要求（如判定存储设备属于当前保护模式指定的设备类型）后向计算机设备发送可以枚举信号，此时计算机设备才会发起枚举动作，以获取存储设备中的数据信息。
15 中间设备基于当前保护模式，将存储设备的数据信息进行保护处理，将保护处理后的存储设备的数据信息反馈给计算机设备，以便建立计算机设备与存储设备间的通信连接。

在一些实施例中，若所述目标设备为具有保护模块的存储设备，所述步骤 S301 之前，还包括：
20

在所述存储设备接入所述计算机设备时，检测与所述计算机设备之间的通信连接请求。

在本实施例中，当存储设备与计算机设备进行物理连接后，为了实现两者间的数据交互，则计算机设备向存储设备发送通信连接请求，或者存储设备向计算机设备发送通信连接请求，并通过该存储设备上的保护模块监听该
25 通信连接请求。

需要说明的是，由于存储设备可能因某些原因被其他方式植入了木马病

毒等恶意程序，而存储设备自身在未上电状态时并未发现该恶意程序，所以在存储设备与计算机设备进行物理连接，使得存储设备上电后，为保证计算机设备的安全性，监听计算机设备与存储设备之间的通信连接请求，以便于后续识别存储设备。

5 在一些实施例中，所述步骤 S301 之后，还包括：

若所述设备类型为预设禁止通信类型，则中断所述通信连接请求。

在本实施例中，预设禁止通信类型包括但不限于人体学接口设备(HID)、具有大容量存储设备(Mass Storage)和 HID 的复合设备或其他功能的复合设备类型。其中，人体学接口设备是一种设备类定义，HID 设备如键盘、鼠标、游戏控制器、操作杆、条码读取器、耳机/扬声器上的音量控制、辅助显示10 器、传感器等。可选地，若所述设备类型为预设禁止通信类型，还反馈拦截信息，该拦截信息用于提示存储设备为禁止通信设备。

可选地，拦截信息用于指示计算机设备通过盘符字符串进行提示，例如，计算机设备上显示接入的设备名为“非法设备”。目标设备上设有指示灯，拦截15 信息可以通过指示灯进行展示，例如指示灯闪烁（或者亮红灯等方式）表示当前接入的存储设备为禁止接入设备。

需要说明的是，本实施例通过验证存储设备的设备类型能够避免非法设备伪装成键鼠设备等接入到计算机设备，以避免非法设备对计算机设备造成安全风险，提高计算机设备的安全性。

20 在一些实施例中，所述步骤 S302，包括：

将所述存储设备的目标硬件特征参数发送至所述计算机设备，所述目标硬件特征参数用于建立所述计算机设备与所述存储设备之间的通信连接。

在本实施例中，对于目标设备为中间设备时，获取存储设备的目标硬件特征参数，并将该目标硬件特征参数转发至计算机设备；对于目标设备为具25 有保护模块的存储设备时，将其预存的目标硬件特征参数发送至计算机设备。

可选地，硬件特征参数是用于表征存储设备特征参数，其包括但不限于设备厂商与产品 ID、设备属性、接口使用的类（例如大容量存储设备）、

端点属性（例如批量传输）、字符串、传输速率、用电需求等。在设备接入时需要验证硬件特征参数，当判定硬件特征参数符合建立通信连接的要求时，计算机设备根据硬件特征参数与存储设备建立通信连接。

在一实施例中，目标硬件特征参数可以为从存储设备直接获取的硬件特征参数；在另一实施例中，目标硬件特征参数可以为对存储设备直接获取的硬件特征参数进行筛选后的特征参数；在又一实施例中，目标硬件特征参数可以为与存储设备直接获取的硬件特征参数匹配的预设硬件特征参数。在又一实施例中，目标硬件特征参数还可以由保护模块直接进行预设。

在一些实施例中，所述将所述存储设备的目标硬件特征参数发送至所述计算机设备，包括：

根据所述存储设备的设备类型，从预设的参数模板中，获取与所述设备类型对应的目标硬件特征参数。

将所述目标硬件特征参数发送至所述计算机设备。

在本实施例中，根据存储设备的设备类型从预设的参数模板中，获取对应于该设备类型的预设硬件特征参数，将该预设硬件特征参数替代从存储设备获取的硬件特征参数，以作为目标硬件特征参数。可选地，预设的参数模板包括有对应于不同设备类型的能够被计算机读取并允许建立通信的预设硬件特征参数。

需要说明的是，本实施例根据对应于设备类型的硬件特征参数，对存储设备的硬件特征参数进行替换修改，以在接入计算机设备进行枚举时，可以保护存储设备的硬件特征参数不被采集，从而实现安全接入的同时，保护存储设备的隐私性。

在另一些实施例中，所述将所述存储设备的目标硬件特征参数发送至所述计算机设备，包括：

获取所述存储设备的硬件特征参数；

根据预设的参数类型，对所述硬件特征参数进行筛选，以确定与所述参数类型对应的目标硬件特征参数；

将所述目标硬件特征参数发送至所述计算机。

在本实施例中，通过对硬件特征参数进行筛选，以保留预设参数类型对应的目标硬件特征参数，并将筛选出的符合预设参数类型的目标硬件特征参数发送至计算机设备，其他参数作为未知参数不予发送至计算机设备，以避免将存储设备的非法参数发送至计算机设备，从而保证计算机设备的数据安全5 性。

为避免将存储设备的非法参数发送至计算机设备，从而保证计算机设备的数据安全性，本申请实施例提供一种机制，对存储设备的特征参数进行模拟，即本实施例提供的所述方法还可包括如下步骤：

10 步骤 11、所述计算机设备与所述存储设备通过所述保护模块建立通信连接之前，模拟所述计算机设备的控制指令，以获取所述存储设备的第一特征参数；

步骤 12、基于所述第一特征参数，判定所述存储设备是否是所述当前保护模式指定的设备类型；若是，执行步骤 13；若否，执行步骤 15（见下文）；

15 步骤 13、基于所述第一特征参数，生成模拟所述存储设备的第二特征参数；

步骤 14、将所述第二特征参数发送至所述计算机设备，以便建立所述计算机设备与所述存储设备间的通信连接。

20 其中，上述步骤 13 中“基于所述第一特征参数，生成模拟所述存储设备的第二特征参数”，包括：

131、获取预设的参数模板；根据所述第一特征参数反映出的所述存储设备的设备类型，从所述预设的参数模板中获取能表征所述设备类型设备的至少一个参数项，以得到所述第二特征参数；或者

25 132、对所述第一特征参数中的参数项进行筛选，基于筛选出的至少一个参数项作，得到所述第二特征参数。

上述参数模板替换进一步保护计算机设备和硬件特征。即在正式接入计算机之前，使用参数模板替换或筛选。使用固定的模板，可以防止接入的存

储设备的硬件描述符出现恶意或未知的、存在风险的参数，攻击计算机。例如，存储设备可能带有恶意的硬件参数，在计算机接入时，有缓冲区溢出漏洞的安全软件在检测描述符时，可能会执行这个带有恶意的硬件参数中含有的恶意指令。通过对参数特征的替换，也可以将接入存储设备的厂商 ID、设备 ID、字符串等硬件参数值通过保护模块进行修改，在接入后计算机设备在 USB1 中读取到的是修改后的参数。这种通常有两种使用场景：一是保护存储设备的硬件特征参数不泄露，例如厂商 ID、设备 ID、字符串等；二是一些计算机设备安全软件可以识别到保护模块的存在，并进行 USB 设备的接入控制，非特定的 USB 硬件参数不允许接入，将保护模块设置硬件参数进行接入放行，可以强制存储设备的接入必须通过保护模块才能接入计算机设备，不允许存储设备直接进行接入，从而保护计算机设备的数据安全。

本实施例提供的所述方法还包括：

- 步骤 15、基于所述第一特征参数判定所述存储设备不是所述当前保护模式指定的设备类型时，终止与所述存储设备的通信；
- 步骤 16、向所述计算机设备发送第一信息，以便所述计算机设备基于所述第一信息显示虚拟盘标识和/或非正常设备提示信息；

其中，若显示有虚拟盘标识，所述第一信息还包含有所述第一特征参数对应的文本，所述文本在所述虚拟盘标识对应的根文件夹中保存。

- 这里需要补充的是：上述步骤 11~16 可以是计算机设备与保护模块间的交互过程中的枚举阶段中的步骤。当然，在枚举阶段除对存储设备的第一特征参数进行保护性处理外，还可对给存储设备的第一存储信息相关参数进行保护性处理。此部分内容采用技术点拆解的方式，对单技术点进行的说明。下文中将有一个整体的实施例，对本申请实施例提供的方案进行详细说明。例如，所述计算机设备与所述保护模块间的交互过程包括：准备阶段、枚举阶段和数据交换阶段；根据所述目标设备的当前保护模式，对所述计算机设备发送的数据交互指令进行权限控制，若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应，为所述数据交互阶

段中的步骤。

在一些实施例中，在图 1 所示实施例的基础上，图 4 示出了步骤 S101 的具体流程示意图。如图 4 所示，步骤 S101 包括：

步骤 S401，识别所述数据交互指令的指令类型；

- 5 步骤 S402，若所述指令类型为所述权限要求对应的预设指令类型，则判定所述数据交互指令满足所述当前保护模式对应的权限要求。

在本实施例中，指令类型包括计算机设备发送的用于读取存储设备中的数据的数据读取指令，或者用于向存储设备中的目标位置写入数据的数据写入指令。可选地，通过保护模块基于预设解析规则，对数据交互指令进行解
10 析，以识别出数据交互指令的实际交互功能，并根据实际交互功能确定指令类型，从而能够以指令类型为识别依据，直接有效的针对计算机设备发送的数据交互指令进行权限控制，避免数据交互指令通过伪装等方式对存储设备进行非法读写，从而提高存储设备的安全性。

示例性地，当前保护模式是针对文件 A 的只读模式，只读模式对应的指令
15 类型应当为数据读取指令，所以若指令类型为针对文件 A 的数据写入指令，则该指令类型无法满足当前保护模式的权限要求；若指令类型为针对文件 A 的数据读取指令，则该指令类型满足当前保护模式的权限要求。

在一些实施例中，在图 1 所示实施例的基础上，所述保护模式为只读模式，图 5 示出了第三实施例的数据安全保护方法的流程示意图。与图 1 相同
20 的步骤不再赘述。如图 5 所示，所述方法还包括：

步骤 S501，响应于所述计算机设备发送的参数读取请求，将只读参数返回至所述计算机设备，所述只读参数用于使所述计算机设备将所述存储设备识别为只读设备。

在本实施例中，只读参数用于使计算机设备将存储设备识别为只读设备。
25 示例性地，当计算机设备与存储设备建立通信连接后，向存储设备读取设备的读写状态时，在只读模式下，目标设备向计算机设备反馈只读参数，以表示存储设备为只读设备，从而使计算机设备识别为只读设备，并使得计算机

设备在正常情况下仅会向存储设备发送数据读取指令，而减少发送除数据读取指令之外的其他无效指令。

可选地，上述只读模式可以兼容其他读写模式，例如全盘只读模式，特定文件读写模式下的只读模式，限位读写模式下的只读模式，以及文件限制

5 读写模式下的只读模式中的任意一种。

只读模式具体实现效果：

让计算机设备识别为只读设备，当计算机发送获取设备读写状态的请求时，保护模块反馈只读状态的参数。例如，计算机设备发送获取存储设备的配置命令（MODE 6）时，保护模块返回存储设备为只读设备的响应信息。计
10 算机设备会在驱动层将设备设置为只读设备，不允许数据写入。

具体的，在保护模块收到计算机设备发送的 SCSI（一种智能的通用接口标准）或 UFI（命令块协议）命令为 0x1A（MODE 6）的请求时，回复带有只读状态的参数数据。例如，作为普通的存储设备（如 U 盘）会回复“0x03 0x00 0x00 0x00”状态为可读可写。在只读保护模式下，将第 2 位（从 0 位起计算）
15 替换为 0x08，回复“0x03 0x00 0x08 0x00”。在计算机设备识别后，将其设置为只读设备，例如界面没有创建文件夹的按钮、计算机设备的文件无法拖曳复制到存储设备中。

使计算机设备无法发送写数据指令。保护模块对计算机设备发送的所有通信命令进行白名单过滤，只允许相关初始化、读数据有关的信息转发至存储设备。其他非白名单（例如 SCSI 或 UFI 命令编码为 0x28（写指令））的信息直接丢弃；或者禁止写操作（例如 SCSI 或 UFI 命令编号为 0x28（写指令））的信息发送至存储设备，保证存储设备在通信层始终不可写状态，有效防止恶意软件绕过操作系统的限制，向存储设备强行写入数据。
20

图示 6a 示出了 U 盘无限制（可读可写）状态下的一个示例图。在无限制
25 （可读可写）状态下，可以对磁盘中的文件内容进行删除、新增和编辑。例如图 6a 说示的，有选择“新建”文件的菜单按钮，并可以选择创建的文件。

图 6b、6c 和 6d 示出了全盘只读模式对应的示例图。参见图 6b 所示，在

全盘只读模式下（中间设备将接入的移动存储介质设置为只读），调出的菜单中（如点击鼠标右键等），菜单中没有“创建”文件的菜单按钮。如图 6c 所示，在全盘只读模式下，调出的菜单中也没有了“删除”菜单按钮。在全盘只读模式下，也无法对文件进行编辑和写入，参见图 6d 所示，显示提示窗口。图 5 6b、6c 和 6d 对应的示例，是在操作系统层面的，根据只读参数进行的只读配置。如果用户强行写入，保护模块也对写入的数据交互指令进行拦截。全盘只读的“全盘”有比较特殊的含义，并非指真的整个硬盘，而是指接入数据源的“全盘”，例如在以下逻辑分盘和特定文件夹模式下，也可以设置为只读。

10 在一些实施例中，在图 1 所示实施例的基础上，图 7 示出步骤 S102 的具体步骤示意图。如图 7 所示，所述步骤 S102，包括：

步骤 S601，响应于所述数据交互指令，对所述存储设备中的目标文件进行读写操作，所述读写操作包括读操作和写操作中的至少一种。

15 在本实施例中，读操作包括读取目标文件中的文件数据（即对应扇区地址数据），并向计算机设备返回该文件数据；写操作包括将数据交互指令中携带的数据写入到目标文件中（即对应扇区地址）。目标文件为显示于计算机设备且允许计算机设备读写的文件，其包括但不限于基于扇区映射的特定文件、预设扇区地址对应的文件和具有预设文件特征的文件等。

20 可选地，对于目标设备为中间设备时，若数据交互指令为数据读取指令，则中间设备将满足权限要求的数据读取指令转发至存储设备，以在存储设备中的目标文件进行读操作。对于目标设备为具有保护模块的存储设备时，若数据交互指令为数据读取指令，则存储设备根据该数据读取指令在其目标文件中执行读操作。

25 需要说明的是，本实施例将目标文件作为读写操作的对象，以将计算机设备的读写限制在当前保护模式下的读写范围内，从而实现读写操作的有效控制，提高计算机设备与存储设备的安全性。

在一些实施例中，若所述保护模式为特定文件读写模式，所述步骤 S601，包括：

响应于所述数据交互指令，将所述目标文件的扇区地址映射至目标地址，所述目标文件为显示于所述计算机设备的文件；

基于所述目标地址，对所述目标文件进行读写操作。

在本步骤中，目标文件为特定文件，特定文件为用户预先选定或保护模块自动创建的允许计算机设备读写的文件，其能够在计算机设备上展示给用户。将特定文件映射至目标地址是指将存储设备中的特定文件的扇区地址映射到目标地址。

可选地，目标地址可以是目标设备中的某个扇区地址，也可以是存储设备中与特定文件不同的某扇区地址，或是与目标设备连接的其他存储设备的某个扇区地址，以使计算机设备仅能识别到特定文件的存在（即在计算机设备上仅将特定文件显示给用户），从而只能对特定文件进行读写。可以理解的是，特定文件应做扩大解释，特定文件可以是一个最小层级的文件（例如一个 A.txt 文本文件），特定文件也可以是一个文件夹。

可选地，特定文件可以预先选定，例如用户可以通过具有全局权限的计算机设备对文件进行选定，特定文件也可以是由目标设备自动创建；在一些实施例，可以在将存储设备通过目标设备接入至具有全局权限的计算机设备时，将特定文件放入至目标设备创建的临时扇区区域中以完成文件选定，使得特定文件能够与存储设备建立映射。

特定文件读写模式包括针对特定文件的只读模式、只写模式和可读可写模式中的至少一种。示例性地，若特定文件读写模式为针对特定文件的只读模式，则目标设备对计算机设备发送的数据交互指令的指令类型进行筛选，仅执行数据读取指令，对于数据交互指令中包括读取指令以外的其他类型指令，则不执行该其他类型指令，并向计算机设备反馈已执行完毕的信息。若特定文件读写模式为针对特定文件的可读可写模式，则目标设备对计算机设备发送的数据交互指令中的读取指令和写入指令均予以响应。

示例地，在特定文件读写模式下，准备阶段，目标设备预先读取存储设备的根目录扇区地址区间（包含扇区首地址至尾地址，地址位置的排序可以

非连续)和特定文件的数据扇区地址区间。数据交互阶段,当接收到数据交互指令时,若保护模块分析出该数据交互指令所要读写的扇区地址在根目录地址区间内,则在特定文件对应的地址区间内进行读写,而原根目录的数据无法被访问。

- 5 可选地,特定文件的读写可通过读写限位实现:目标设备通过建立读写限位区域,对于非特定文件的数据区域禁止读取和写入,对于特定文件以外,只允许在空白数据区域写入。

需要说明的是,本实施例通过选定特定文件并映射于目标设备中,以使计算机设备仅能够识别到特定文件的存在,避免计算机设备直接对存储设备
10 中的非特定文件的数据进行读取或写入,从而保护存储设备的数据安全性。

即在当前保护模式为特定文件模式时,本实施例提供的所述方法还包括如下各步骤:

步骤 31、当所述当前保护模式为特定文件模式时,确定所述存储设备中的至少一个特定文件或文件夹;

- 15 步骤 32、获取所述至少一个特定文件或文件夹的地址信息;

步骤 33、建立所述至少一个特定文件或文件夹的地址信息与根目录地址的映射关系。

当设置为特定文件读写时,由使用者先行在存储设备中创建,或保护模块自动在存储设备中创建固定的特定文件夹,并可预先存放需要被计算机设备读取的文件夹或文件数据,使计算机设备能够读取数据、修改数据或拷贝文件,也可以设置为只读模式。当设置为空白文件夹读写时,保护模块在存储设备中自动创建一个新的文件夹,并作为特定文件夹,使计算机设备读取根目录时得到一个“空白盘”的数据。可以使计算机设备智能读写用户允许操作的特定文件或文件夹,或者可以自动创建新的空白文件夹用于计算机设备只
20 能写入新的文件,无法读取已有的文件等。其中,可用空间为实际存储设备的剩余空间。

参见对比图 8,未连接中间设备的存储设备或没有集成保护模块的存储设

备直接接入计算机设备，先显示存储设备根目录下的所有文件。再点击打开“根目录/SAFEDIR.NEW/THEDIR.NEW”文件夹后，显示该文件夹内的文件：THEFILE_1.txt、THEFILE_2.txt。假设采用本申请实施例提供的方案，“根目录/SAFEDIR.NEW/THEDIR.NEW/”文件夹被设置为特定文件夹。存储设备通过保护模块接入计算机设备后，计算机设备上只能显示“根目录/SAFEDIR.NEW/THEDIR.NEW/”文件夹内的文件：THEFILE_1.txt、THEFILE_2.txt的两个文件，其上级目录和其他文件不可显示。

由此可知，本实施例提供的所述方法还可包括如下步骤：

计算机设备与存储设备建立通信后，接收到所述计算机设备请求读取所述存储设备的根目录地址时，基于所述映射关系，确定与所述根目录地址存在映射关系的至少一个特定文件或文件夹的地址信息，以读取所述地址信息对应的数据。

为了方便理解，此处对上文中提及的保护模块建立特定文件夹映射的流程进行说明：

15 1、保护模块预先读取存储设备的信息，获取根目录首扇区地址以及扇区地址集合；

2、如果为特定文件夹模式，则分析根目录扇区地址，按照文件系统协议，根据特定文件夹的文件名、文件路径等文件特征，寻找特定文件夹的首扇区地址以及扇区地址集合；

20 3、如果为空白的特定文件夹模式，则按照文件系统协议，根据预设的文件路径、文件名等规则，创建新的文件夹，并作为特定文件夹的首扇区地址以及扇区地址集合。

4、建立特定文件夹扇区地址（或存储数据空间地址集合）与根目录扇区地址（或存储数据空间地址集合）的映射关系。当计算机设备在请求读取根目录扇区地址数据时，返回映射的特定文件夹扇区对应的地址数据。例如，在 FAT 文件系统中，扇区地址集合为特定文件夹或根目录的簇链对应的所有扇区地址集合。具体的：

4.1、基于扇区地址之间的映射。例如，存储设备的根目录首扇区地址为：17348 扇区。特定文件夹的首扇区地址为：17396 扇区时，当计算机设备发送读取 17348 扇区指令时，保护模块读取存储设备的 17396 扇区数据并返回。

例如，存储设备的根目录的第 2 扇区地址为：17349 扇区。特定文件夹的第 2 扇区地址为：17397 扇区时，当计算机设备发送读取 17349 扇区指令时，保护模块读取存储设备的 17397 扇区数据并返回。

4.2、基于文件分配表的替换。文件分配表是用于记录具体文件内容数据所在扇区地址（具体的记录为文件系统划分的簇或块）的所有集合。一般为链式结构（簇位置固定，上一簇记录下一簇的簇号）。计算机设备基于文件分配表记录的扇区地址进行文件数据的读写。

例如，存储设备的根目录数据记录的地址为：第 3 簇（记录第 4 簇）、第 4 簇（记录第 5 簇）、第 5 簇（记录终止标记）。特定文件夹数据记录的地址为：第 6 簇（记录第 7 簇）、第 7 簇（记录第 8 簇）、第 8 簇（记录终止标记）。当计算机设备发送读取文件分配表扇区数据指令时，保护模块读取存储设备的文件分配表数据，替换为在第 3 簇（记录第 7 簇），返回。例如当计算机读取根目录数据的簇链表第 2 簇时（第一簇的数据可以通过扇区地址之间的映射），直接跳转到特定文件夹数据的簇链（特定文件夹的第 2 簇），进一步读取特定文件夹数据的扇区地址。

4.3、基于文件系统引导信息的替换。文件系统引导信息一般存储有首目录内容数据的地址（例如簇号）。当计算机设备发送读取文件系统引导信息扇区数据指令时，保护模块读取存储设备的引导信息扇区数据，将首目录地址替换为在第 6 簇（记录第 7 簇）并返回，使计算机直接以第 6 簇（特定文件夹数据的起始簇）开始的数据作为根目录数据。

由此可知，所述至少一个特定文件或文件夹的地址信息包括：至少一个特定文件或文件夹的首扇区地址；或者文件分配表中至少一个特定文件或文件夹被记录的簇或块信息。

上述的文件系统引导信息扇区地址、文件分配表扇区地址是基于文件系

统，由保护模块的预先读取存储设备的数据分析得到的。

在一些实施例中，所述目标文件包括所述存储设备已有的特定文件或预设文件，或者在所述计算机设备与所述存储设备建立通信连接前自动生成的文件。

5 在本实施例中，已有的特征文件为固定存在于存储设备的文件，预设文件可以为空白文件，即预设文件中不会显示存储设备中的任何现存数据；预设文件也可以为包含非重要数据的预设文件。预设文件可以在存储设备在接入计算机设备前自动创建，也可以是存储设备原有的空白文件夹，也可以是目标设备生成的临时文件夹。

10 在一种可能实施的方式中，对于预设文件为空白文件，其不存在可读文件数据，所以读取不到相应文件数据。在接收到写入指令时，根据写入指令在空白文件（即对应的扇区地址）写入数据，对于计算机设备在本次数据交互中成功写入到空白文件的数据，其可被计算机设备识别和读取。本实施例通过创建空白文件与目标设备之间的映射，使计算机设备无法读取到存储设备中的原有数据区的文件数据，而对空白文件进行读取与写入，从而限制计
15 算机设备的读写权限，保护存储设备的数据安全性。

 可选地，在向预设文件中写入数据时，计算机设备显示所写入的数据，也可以不显示写入的数据。

 还有如上文中提及到的：当设置为特定文件读写时，由使用者先行在存储设备中创建，或保护模块自动在存储设备中创建固定的特定文件夹。其中，
20 对使用者先行创建不作说明。这里对保护模块自动在存储设备中创建固定的特定文件夹进行说明。即本申请实施例提供的所述方法的执行主体保护模块还具有自动创建特定文件夹的功能。具体的，本实施例提供的所述方法还包括如下步骤：

25 步骤 21、当所述当前保护模式为特定文件模式时，输出是否设置空白文件或文件夹的提示信息；

 步骤 22、响应于用户针对所述设置空白文件或文件夹的提示信息的确认

指令，在所述存储设备中创建一个文件或文件夹，作为所述特定文件模式对应的特定文件或文件夹；

步骤 23、响应于用户针对所述设置空白文件或文件夹的提示信息的否定指令，获取用户指定的至少一个文件或文件夹，将用户指定的至少一个文件
5 或文件夹作为所述特定文件模式对应的特定文件或文件夹。

举一个具体场景，特定文件模式被选中后，该保护模块的载体，如存储设备、中间设备、计算机设备、可信任设备等这些带有交互模块的设备，就会输出是否设置空白文件或文件夹的提示信息。若用户针对该设置空白文件或文件夹的提示信息做出确认指示，则所述存储设备中创建一个文件或文件
10 夹，作为所述特定文件模式对应的特定文件或文件夹。若用户针对所述设置空白文件或文件夹的提示信息触发否定指示，则等待用户指定存储空间中的至少一个文件或文件夹作为所述特定文件模式对应的特定文件或文件夹。

也就是说，在特定文件模式被选中后，保护模块给用户提供了选择创建空白文件作为特定文件或文件夹，还是用户指定文件或文件夹作为特定文件
15 或文件夹的选择机会，保护模块根据用户指令确定存储区域中的所述特定文件模式对应的特定文件或文件夹。当然，保护模块也可随机确定一个已有的文件或文件夹作为特定文件模式对应的特定文件或文件夹。例如，保护模块基于预置的选择策略或算法，自存储空间中选出至少一个符合该策略或算法的文件或文件夹作为特定文件模式对应的特定文件或文件夹；也可以根据预
20 设策略（例如文件路径和文件名），自动完成创建特定文件或文件夹，可以不需要人为干预。其中，本实施例对选择策略或算法的具体实现不作限定。

图 9b 和 9c 示出了特定文件模式下特定文件夹对应的示例图。图 9a 和 9d 示出了全局权限（即未进行特定文件夹映射，未开启特定文件夹模式）视角下可看见的情况，目的是为了产生对比效果，体现本申请方案的区别。参见
25 图 9a，如果在全局权限（即未进行特定文件夹映射，未开启特定文件夹模式）视角下，可以看到根目录下有 SAFEDIR.NEW 文件夹（特定文件夹），文件夹内有 NEWDIR.NEW（空白文件夹根目录）、THEDIR.NEW 文件夹（固定

的特定文件夹)。该文件夹可以由用户创建,也可以由保护模块自动生成。

THEDIR.NEW 文件夹有 2 个文件。如图 9b,在特定文件模式下,映射至固定的特定文件夹,具有保护模块的存储设备或存储设备通过中间设备接入计算机设备后,在计算机设备上只能看到根目录下有 2 个文件(THEDIR.NEW),

5 并且可以读、或写、或读写等等,看不到 SAFEDIR.NEW 文件夹及文件夹内的 NEWDIR.NEW 根目录,也看不到其他文件,包括 U 盘根目录下的其他文件。图 9c 示出了在特定文件模式(映射到固定的特定文件)下,继续新增一个文件 THEFILE_3_NEW.txt 的示例。图 9d 示出了在全局权限(即未进行特定文件夹映射,未开启特定文件夹模式)视角下可以看到 THEDIR.NEW 文件

10 夹内,新增的 THEFILE_3_NEW.txt 文件的情况。

图 10a、10b、10c 和 10d 示出了特定文件模式下空白文件夹为特定文件对应的示例图。如图特定文件模式下特定文件为空白文件夹时,在计算机设备的界面上显示的该 U 盘内为空,如图 10a 所示。当然,该 U 盘是有数据的,只是因为特定文件夹为空白文件夹,映射到该空白文件夹,致使从计算机设备的使用者角度来看该 U 盘内为空,没有数据。图 10b 示出了在当前保护模式为特定文件模式下空白文件夹时,自动创建或用户创建的 NEWFILE_1 文件的情况。图 10b 为 U 盘第一次运行时对应的情况,用户可看见新创建的空白文件。图 10c 示出了在当前保护模式为特定文件模式下空白文件夹时, U 盘第二次运行(即具有保护模块的 U 盘或连接中间设备的 U 盘再次连接计算机设备),上述图 10b 中的 NEWFILE_1 文件看不见了。图 10d 示出了在当前保护模式为特定文件模式下空白文件夹时,自动创建或用户创建的 NEWFILE_2 文件的情况。因为,此次是新创建的,用户是可以看见 NEWFILE_2 文件的。

15

20

图 11a 和 11b 示出了全局权限视角下浏览 NEWFILE_1 文件和 NEWFILE_2 文件,这两个创建的文件对应的目录。参见图 11a 示出的例子,在 U 盘的 NEWDIR.NEW 目录下自动创建了 1.NEW 子目录,并有第 1 次运行“空白文件夹模式”创建的 NEWFILE_1 文件。参见图 11b 示出的例子,在 U 盘的 NEWDIR.NEW 目录下自动创建了 2.NEW 子目录,并有第 2 次运行“空

25

白文件夹模式”创建的 NEWFILE_2 文件。

另外需要说明的是：因为特定文件夹模式，只是将文件夹映射到根目录，不影响原有的存储空间，这与下文中提及逻辑分盘模式不同。逻辑分盘模式在分盘时会对存储设备的存储空间（如可用空间）进行划分。

- 5 在一些实施例中，若所述保护模式为限位读写模式，所述步骤 S601，包括：

响应于所述数据交互指令，基于预设扇区地址区间，对所述数据交互指令对应的目标扇区地址进行验证，所述目标扇区地址为所述存储设备基于所述数据交互指令执行读写操作时的扇区地址；

- 10 若所述目标扇区地址在所述预设扇区地址区间内，则在所述存储设备的目标扇区地址进行读写操作。

通过扇区限位读写模式，对于存储设备用户来说，可以保护存储设备的特定扇区区间的数据不被读取、修改或写入（基于扇区区间）。对于计算机设备用户来说，特定扇区数据无法进行读取，可以保护计算机设备免遭恶意数据的攻击。

15

具体实现方式为：

计算机设备向保护模块发送读取扇区数据或写入扇区数据的交互指令时，保护模块判断该交互指令操作的扇区地址是否符合预设的特定扇区区间规则，如果符合就执行，如果不符合就不执行。

- 20 另外，在不符合的情况下，必然会响应写入或读出的失败状态。计算机设备会认为存储设备存在问题继而反复进行无效的操作。为此，保护模块可以返回执行成功的响应、响应空白数据、响应其他非真实的数据，使计算机认为执行成功。实际上保护模块没有真正的操作存储设备的数据，防止计算机设备认为操作失败，不断尝试操作。

- 25 上述特定扇区区间规则的设置。一种可实现的技术方案是，特定扇区区间可以人工预先设置，例如设置 0~9999 扇区区间只读，50000~69999 扇区区间只能写入，80000~99999 扇区区间不可读也不可写，其他扇区区间可读可写。

另一种可实现的技术方案是：特定扇区区间也可以是通过保护模块或外部设备自动设置的。例如，在进一步保护特定文件数据的读写权限时（例如在准备阶段）：

一、建立存储设备引导区、文件系统引导区的保护扇区地址区间。保护
5 模块预先读取存储设备，寻找存储设备引导区、文件系统引导扇区区间，建立对应的扇区区间集合，并设置该扇区区间为只读权限。防止计算机恶意写入破坏其数据，导致文件数据无法被正常读取。

二、建立特定文件夹、文件的保护扇区地址区间。保护模块预先读取存储设备，通过对特定文件、文件夹的文件数据特征或文件属性（例如文件类型）特征进行判断，再根据文件系统规则寻找特定文件、文件夹对应的扇区地址数据，并建立对应的特定文件数据扇区区间数据集合。并设置该扇区集合可读可写权限，在文件系统数据区（文件系统引导区除外）的扇区地址不能读写权限。防止非特定文件夹数据被通过扇区扫描（从 0 扇区至结尾扇区）的方式读取到。

15 三、建立未使用扇区地址的可读写保护区间。保护模块预先读取存储设备，通过文件系统的规则，分析出未分配使用的扇区地址区间。例如，在 FAT 文件系统中（包括 FAT32、exFAT 等），读取文件分配表的未分配使用的簇号，可以进一步转换未分配使用扇区地址区间的集合。并设置可读写权限，在特定文件夹模式中，可以使计算机创建文件和写入数据；也可以设置为只写权限，也防止读取未分配使用扇区地址的旧数据（例如已删除的文件数据）。
20 其中，文件删除原理大体为：计算机设备一般只会将删除的文件标记为删除状态，并将数据存储的空间标记为未分配使用（例如清空簇链），但是存储空间的数据仍存在，如果没有被覆盖写入，删除文件的数据可以被读出。

在本实施例中，限位读写模式包括针对预设扇区地址区间内的文件的只
25 读模式、只写模式和可读可写模式。预设扇区地址区间包括允许计算机设备读写的所有扇区地址，其可以预先设置得到。

可选地，保护模块对数据交互指令中所要执行读写操作的目标扇区地址

进行识别，并在该目标扇区地址在预设扇区地址区间内时，执行读写操作，从而控制计算机设备可以读写数据的扇区地址，以保护存储设备的数据安全性。例如，数据交互指令所要读写的文件的目标扇区地址为存储设备的第 0 至 499 扇区，若当前限位读写模式仅允许读写存储设备的第 500 至 999 扇区，
5 则目标扇区地址不在预设扇区地址区间内，若当前限位读写模式允许读写存储设备第 0 至 499 扇区，则目标扇区地址在预设扇区地址区间内。

需要说明的是，本实施例通过限位读写模式，能够将存储设备允许的读写范围限制在预设扇区地址区间内，以满足在某些需要限位读写的场景。

在一些实施例中，在所述保护模式为文件限制读写模式时，所述步骤 S601，
10 包括：

响应于所述数据交互指令，基于预设文件特征，对所述数据交互指令对应的目标文件特征进行验证，所述目标文件特征为所述存储设备基于所述数据交互指令执行读写操作时对应的文件特征；

若所述目标文件特征符合所述预设文件特征，则对所述存储设备中的所述目标文件进行读写操作。
15

通过文件限制读写模式，限制计算机设备向存储设备读取或写入符合预设规则的文件，文件的预设规则有文件名、文件类型（如文件名命名规则、文件后缀、文件内容对应的特定位置的特征值等）。

对于存储设备使用人来说，可以保护存储设备的特定文件类型文件的数
20 据不被读取（例如只能读取DOC文档，或者禁止读取PDF类型的文件）、修改（例如只能修改DOC文档，或者禁止读取PDF类型的文件）、删除（例如禁止删除DOC文档，或者只能删除PDF类型的文件）、创建（例如禁止写入文件类型为EXE可执行文件类型的文件，只能创建DOC文档）。对于计算机设备使用人来说，可以保护计算机设备免遭恶意程序的攻击，例如日常工作
25 场景只需要拷贝PDF和DOC文件，仅允许读取或写入存储设备的PDF和DOC格式的文件，其他文件类型（如EXE可执行文件）禁止读取，避免先进的木马病毒文件绕过安全软件限制，攻击计算机设备。

具体实现方法：

1、在限制计算机设备读取（包括复制）或修改文件内容数据时：

1.1、寻找需要控制的文件。保护模块在存储设备中，预先寻找出禁止访问或者允许访问的文件，以及文件内容数据对应的扇区地址区间（例如首扇区等）。
5

1.2、判断读写数据交互指令。当计算机的交互指令为读写控制文件的扇区地址时，根据可读、或者可写权限做出判断。

1.3、根据设置的权限做出响应。在扇区地址具有读或写权限时，读取或写入存储设备对应扇区的数据并返回；在扇区地址禁止读或写时，可以返回错误的状态响应，也可以返回执行成功的响应、或者响应空白数据、或者响
10 应其他非真实的数据，使计算机认为执行成功，实际上保护模块没有真正的操作存储设备的数据，防止计算机设备认为操作失败，不断尝试操作。

即上述过程可总结为：

所述数据交互指令满足所述当前保护模式对应的权限要求，且所述数据交互指令为读取或修改文件内容数据时，确定扇区地址，读取或写入存储设备对应扇区的数据并返回；
15

所述数据交互指令不满足所述当前保护模式对应的权限要求时，返回错误的状态响应、或返回执行成功响应、或响应空白数据、或将预设数据作为反馈数据进行响应。

20 2、在限制计算机设备创建新文件、删除文件或修改文件属性时：

2.1、寻找文件夹数据扇区地址集合（例如在准备阶段）。保护模块在存储设备中的情况，预先寻找根目录，读取根目录下子目录和文件信息，基于子目录继续读取下级目录和文件信息，直至找出具有需要控制的文件夹（可以为至少一个特定文件、特定文件夹集合或包括根目录的全部文件夹），以及文件夹数据对应的扇区地址区间（例如首扇区等）。
25

2.2、判断读写数据交互指令。当计算机设备写入的扇区地址为文件夹数据地址时，对比读取存储设备对应的扇区地址的数据，判断计算机设备操作

的动作（创建文件、修改文件属性、删除文件）和文件类型（根据文件名规则、文件后缀、文件具体数据等）。例如：

计算机设备写入的数据为包含文件信息的 A.txt、B.txt、C.txt 三个数据，但是存储设备对应扇区地址现有的数据为 A.txt、B.txt,则判断计算机设备要将

5 创建 C.txt 文件；

计算机设备写入的数据为包含文件信息的为 A.txt、B.txt（标记为删除状态），或者写入的数据为仅包含文件信息的为 A.txt，则判断计算机设备要将删除 B.txt 文件；

计算机设备写入的数据为包含文件信息的为 A.txt、C.txt（文件其他属性不变），或写入的数据为包含文件信息的为 A.txt、B.txt（删除状态）、C.txt(其
10 他文件属性与 B.txt 一致)，则判断计算机设备要将 B.txt 文件名修改为 C.txt；

计算机设备写入的数据为包含文件信息的为 A.txt、B.txt（文件创建时间等数据与存储设备现有的数据不一致），则判断计算机设备要将修改 B.txt 的文件属性信息。

15 具体的，表 3-表 6 的判断创建文件、判断删除文件、判断修改文件名、判断修改文件属性示例所示。例如：保护模块先预先记录 showdir 文件夹（可
以为至少一个或多个或全部文件夹，包括根目录等）扇区地址集合（至少一个扇区地址）。当计算机发送的数据交互指令匹配到 showdir 文件夹的扇区地址集合时，保护模块在执行写入操作前，前预先读取对应扇区数据进行对比
20 判定，并根据保护模式的预设执行下一步操作。

表 3、判断创建文件示例

1.保护模块预先记录 showdir 文件夹扇区地址集合	记录的扇区地址集合包括： 0x00010038	设置需要进行文件操作识别的扇区地址集合
2. 计算机设备发送的数据交互指令	写入扇区地址包括：0x00010038 写入扇区地址 0x00010038 的数据为： 2e2020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e20202020202020201000a5f5b3	命中识别的扇区地址 写入的数据有： <u>A.txt</u> 、 <u>B.txt</u> 、 <u>C.txt</u> 共 3 个文件数据

	a856a8560000f6b3a856000000000000 42202020202020205458542010a10ab4 a856a8560000cdb3a8561c0007000000 41202020202020205458542010a40ab4 a856a8560000c8b3a8561d0006000000 432020202020202054585420109a8cb4 a856a85600008db4a85626000d000000 000000000000000000000000000000 ...空字节至 512 字节	
3.保护模块在执行写入操作前,预先读取对比数据	读取扇区地址包括: 0x00010038; 扇区地址 0x00010038 的数据为: 2e20202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e202020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000 42202020202020205458542010a10ab4 a856a8560000cdb3a8561c0007000000 41202020202020205458542010a40ab4 a856a8560000c8b3a8561d0006000000 000000000000000000000000000000 ...空字节至 512 字节	对比数据有: <u>A.txt</u> 、 <u>B.txt</u> 共 2 个文件 对比结果: 在原存储扇区空间 (或 showdir 文件夹) 将新增 C.txt 文件数据
4.保护模块判定操作	计算机设备要向 showdir 文件夹中创建 C.txt 文件	
5.保护模块根据保护模式执行下一步操作: 是否允许创建等, 或者触发其他保护模式等		

表 4、判断删除文件示例

1. 保护模块预先记录 showdir 文件夹扇区地址集合	记录的扇区地址集合包括: 0x00010038	设置需要进行文件操作识别的扇区地址集合
2. 计算机设备向保护模块发送的数据交互指令(类型 1)	写入扇区地址包括: 0x00010038 写入扇区地址 0x00010038 的数据为: 2e20202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e202020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000 e5202020202020205458542010a10ab4 a856a8560000cdb3a8561c0007000000 41202020202020205458542010a40ab4 a856a8560000c8b3a8561d0006000000 432020202020202054585420109a8cb4 a856a8560000d1b3a85626000d000000	命中识别的扇区地址 写入的数据有: <u>A.txt</u> 、 <u>C.txt</u> 共 2 个正常文件数据, 1 个标记为删除 (0xE5) 的文件数据

	00000000000000000000000000000000 ...空字节至 512 字节	
2. 计算机设备向保护模块发送的数据交互指令(类型 2)	写入扇区地址包括: 0x00010038 写入扇区地址 0x00010038 的数据为: 2e20202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e202020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000 <u>4120202020202020205458542010a40ab4</u> <u>a856a8560000c8b3a8561d0006000000</u> 43202020202020202054585420109a8cb4 <u>a856a8560000d1b3a85626000d000000</u> 00000000000000000000000000000000 ...空字节至 512 字节	命中识别的扇区地址 写入的数据有: <u>A.txt</u> 、 <u>C.txt</u> 共 2 个文件数据
3. 保护模块在执行写入操作前, 预先读取对比数据	读取扇区地址包括: 0x00010038; 扇区地址 0x00010038 的数据为: 2e20202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e202020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000 <u>4220202020202020205458542010a10ab4</u> <u>a856a8560000cdb3a8561c0007000000</u> <u>4120202020202020205458542010a40ab4</u> <u>a856a8560000c8b3a8561d0006000000</u> 43202020202020202054585420109a8cb4 a856a85600008db4a85626000d000000 00000000000000000000000000000000 ...空字节至 512 字节	对比数据有: <u>A.txt</u> 、 <u>B.txt</u> 、 <u>C.txt</u> 共 3 个文件数据 对比结果: 在原存储扇区空间 (或 showdir 文件夹) 的 B.txt 文件将被标记为删除 (类型 1) 或者 B.txt 文件数据被清空 (类型 2)
4. 保护模块判定	计算机设备要在 showdir 文件夹中删除 B.txt 文件	
5. 保护模块根据保护模式执行下一步操作: 是否允许删除, 或者触发其他保护模式等		

表 5、判断修改文件名示例

1. 保护模块预先记录 showdir 文件夹扇区地址集合	记录的扇区地址集合包括: 0x00010038	设置需要进行文件操作识别的扇区地址集合
2. 计算机设备向保护模块发送的数据交互指令	写入扇区地址包括: 0x00010038 写入扇区地址 0x00010038 的数据为: 2e20202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e202020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000	命中识别的扇区地址, 写入的数据有: <u>A.txt</u> 、 <u>C.txt</u> 共 2 个文件数据

	<u>4320202020202020545854201095d31d</u> <u>a956a9560000cdb3a856370007000000</u> <u>4120202020202020545854201098d31d</u> <u>a956a9560000c8b3a856380006000000</u> 00000000000000000000000000000000 ...空字节至 512 字节	
3. 写入前预先读取对比数据	读取扇区地址包括：0x00010038； 扇区地址 0x00010038 的数据为： 2e20202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e202020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000 <u>4220202020202020545854201095d31d</u> <u>a956a9560000cdb3a856370007000000</u> <u>4120202020202020545854201098d31d</u> <u>a956a9560000c8b3a856380006000000</u> 00000000000000000000000000000000 ...空字节至 512 字节	对比数据有： <u>A.txt</u> 、 <u>B.txt</u> 共 2 个文件数据 对比结果：在原存储扇区空间（或 showdir 文件夹）的 B.txt 文件信息要被清除，并添加了 C.txt 文件信息。C.txt 文件信息除了文件名与原文件 B.txt 不一致外，其他信息一致。
4. 判定计算机设备操作	将 B.txt 文件的文件名修改为 C.txt	
5. 根据保护模式执行下一步操作：是否允许修改文件名，或者触发其他保护模式等		

表 6、判断修改文件属性示例

1. 保护模块预先记录 showdir 文件夹扇区地址集合	记录的扇区地址集合包括： 0x00010038	设置需要进行文件操作识别的扇区地址集合
2. 计算机设备向保护模块发送的数据交互指令	写入扇区地址包括：0x00010038 写入扇区地址 0x00010038 的数据为： 2e20202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e202020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000 <u>4120202020202020545854201063b2b5</u> <u>a856a8560000c8b3a856270006000000</u> <u>4220202020202020545854201068b2b5</u>	命中识别的扇区地址， 写入的数据有： <u>A.txt</u> 、 <u>C.txt</u> 共 2 个文件数据

	<u>a856a856000095b6a8562e000a000000</u> <u>00000000000000000000000000000000</u> ...空字节至 512 字节	
3. 写入前预先读取对比数据	读取扇区地址包括：0x00010038； 扇区地址 0x00010038 的数据为： 2e202020202020202020201000a5f5b3 a856a8560000f6b3a8561b0000000000 2e2e2020202020202020201000a5f5b3 a856a8560000f6b3a856000000000000 <u>4120202020202020545854201063b2b5</u> <u>a856a8560000c8b3a856270006000000</u> <u>4220202020202020545854201068b2b5</u> <u>a856a8560000cdb3a8562e0007000000</u> <u>00000000000000000000000000000000</u> ...空字节至 512 字节	对比数据有： <u>A.txt</u> 、 <u>B.txt</u> 共 2 个文件数据 对比结果：在原存储扇区空间（或 showdir 文件夹）的 B.txt 文件属性要被修改，修改的属性为文件大小和修改时间。修改文件大小和修改时间属性，可能要进行文件数据修改
4. 判定计算机设备操作	修改 B.txt 文件的文件属性，进一步判断为要修改文件数据	
5. 根据保护模式执行下一步操作：是否允许修改文件属性或数据，或者触发其他保护模式等		

即上述过程可总结为：

所述数据交互指令满足所述当前保护模式对应的权限要求，且所述数据交互指令为创建新文件、删除文件或修改文件时，

5 确定扇区地址；

若所述数据交互指令包含多个文件的信息，所述存储设备对应的所述扇区地址含有所述多个文件中的部分文件，则确定所述计算机设备要在所述扇区地址创建至少一个文件；其中，创建的至少一个文件为所述多个文件中除已有的部分文件之外的剩余文件；

10 若所述数据交互指令包含多个文件的信息，且所述多个文件中至少部分文件带有删除标记，则查找所述存储设备对应所述扇区地址内与所述多个文件中带有删除标记的部分文件关联的至少一个预删除文件；确定所述计算机

设备要将所述至少一个预删除文件删除；

若所述数据交互指令包含第一文件集合，所述存储设备对应的所述扇区地址含有第二文件集合，且所述第一文件集合为所述第二文件集合的子集，则确定所述计算机设备要将所述第二文件集合中不属于所述第一文件集合的

5 至少一个文件删除；

若所述数据交互指令包含的第一文件的除文件名外的属性信息与所述存储设备对应的所述扇区地址内的第二文件的除文件名外的属性信息相同，则确定所述计算机设备要将所述扇区地址内的所述第二文件的文件名修改为所述第一文件的文件名；

10 若所述数据交互指令包含的第一文件的文件名与所述存储设备对应扇区地址内的第二文件的文件名相同，且所述第一文件的除文件名外的属性信息与所述第二文件的除文件名外的属性信息不同，则确定所述计算机设备要将所述第二文件的除文件名外的属性信息修改为所述第一文件的除文件名外的属性信息。

15 这里需要补充的：在修改的属性信息可以为文件大小、时间等属性，还可能要进行文件数据的修改。即上述步骤“若所述数据交互指令包含的第一文件的文件名与所述存储设备对应扇区地址内的第二文件的文件名相同，且所述第一文件的除文件名外的属性信息与所述第二文件的除文件名外的属性信息不同，则确定所述计算机设备要将所述第二文件的除文件名外的属性信息

20 修改为所述第一文件的除文件名外的属性信息”，可具体为：

若所述数据交互指令包含的第一文件的文件名与所述存储设备对应扇区地址内的第二文件的文件名相同，且所述第一文件的除文件名外的属性信息与所述第二文件的除文件名外的属性信息不同，则确定所述计算机设备要将所述第二文件的除文件名外的属性信息修改为所述第一文件的除文件名外的

25 属性信息；

若计算机设备要修改的属性信息包括文件大小和时间，则确定计算机设备要修改所述第二文件的文件数据。

3、根据预设的权限做出响应。

即本申请实施例提供的所述方法还包括如下步骤：

基于当前保护模式，对所述计算机设备要执行的操作进行权限判定或触发其他保护模式。

5 例如，在确定计算机设备要在所述扇区地址创建至少一个文件时，保护模块基于当前保护模式判定是否允许创建，或触发其他保护模式。

在确定所述计算机设备要将所述至少一个预删除文件删除或确定所述计算机设备要将所述第二文件集合中不属于所述第一文件集合的至少一个文件删除时，保护模块基于当前保护模式判定是否允许删除，或触发其他保护模
10 式。

确定所述计算机设备要将所述扇区地址内的所述第二文件的文件名修改为所述第一文件的文件名时，保护模块基于当前保护模式判定是否允许修改文件名，或触发其他保护模式。

确定所述计算机设备要将所述第二文件的除文件名外的属性信息修改为
15 所述第一文件的除文件名外的属性信息和/或修改所述第二文件的文件数据时，保护模块基于当前保护模式判定是否允许修改属性信息和/或修改文件数据，或触发其他保护模式。

其中，上文中触发的其他保护模式可以是与当前保护模式组合在一起的至少一个保护模式，如加密写入模式、人工确认模式等等。

20 在写入的文件类型具有创建文件、修改文件属性、删除文件等限制时：
一是，可以返回错误的状态响应，也可以返回执行成功的响应，或者响应空白数据、或者响应其他非真实的数据（例如计算机进一步读取验证时，保护返回其写入的数据），使计算机设备认为执行成功，实际上保护模块没有真正的操作存储设备的数据，防止计算机设备认为操作失败，不断尝试操作。
25 二是，无权限创建文件时，在文件夹数据中正常写入，但是写入的文件内容数据为非真实数据，使计算机设备认为执行成功，存储设备也真实创建该文件，但是文件的内容数据非真实，可以避免恶意代码的执行，防止计算机设

备认为操作失败，不断尝试操作。响应还可以包括人工确认模式、加解密模式、文件异常模式等至少一种保护模式的判断。

其中，在限制计算机设备读取文件夹中的文件属性数据时：按照文件读取规则，判断数据交互指令。在存储设备中的文件不符合文件读取规则时，

5 向计算机设备响应非真实的数据，将文件在计算机设备中进行隐藏，例如：一是将文件属性替换为已删除状态，向计算机设备返回，以使计算机设备认为文件已删除，不再显示；二是将文件属性中的首扇区地址（或者文件系统中称的首簇、首块）替换为 0x00、文件大小替换为 0 字节，使计算机设备无法直接读取到文件的数据；三是可以以空白数据等非真实的数据代替文件对

10 应的数据，使计算机设备无法读取真实的数据，防止计算机设备认为操作失败，不断尝试操作。使计算机设备无法读取文件的正确属性，无法在计算机上进行显示，以及进一步文件内容数据的读取等操作。

在本实施例中，文件限制读写模式包括针对具有预设文件特征的文件

15 的只读模式、只写模式和可读可写模式。预设文件特征是指预先配置的允许计算机设备进行读写的文件所具有的特征参数，其包括但不限于文件名称、文件后缀、文件类型、文件大小、文件内容数据中预设扇区数据对应的哈希值、文件中预设扇区数据中特定位置对应预设的字节值（类似关键字比对命中的，比如判断第 5 页第 10 个字是否为 0x88，相当于：判断第 5 扇区第 10 个字节为 0x88）等文件特征。可选地，通过预设黑名单文件特征或白名单特征，禁

20 止或允许对应文件的读写。例如，若文件限制读写模式具体为针对 PDF 文件类型的只读模式，则在执行读操作时，只读取存储设备中的 PDF 文件，其他文件类型无法被读取。

示例性地，当存储设备与计算机设备建立通信时，目标设备按照对应文件系统的预设规则，自动爬取存储设备内允许被计算机设备访问的所有文件

25 的属性（如文件名、起始扇区地址等），并建立文件唯一标识和起始扇区地址的对应关系。对于读操作：当计算机设备读取扇区地址为某个文件的起始地址时，则认为要读写该文件，则查询该文件是否具备预设文件特征。对于

读操作：当计算机设备写入某个文件时，先将该文件的属性（文件名、起始扇区地址等）更新写入至对应的文件夹数据，通过写入的文件夹数据进行比对，判断出所要写入的文件的属性，再判断该文件是否具备预设文件特征。

需要说明的是，本实施例通过文件限制读写模式，以满足用户希望计算机设备只能读取具有预设文件特征的文件场景需求，从而提高存储设备的数据安全性。

在一些实施例中，所述预设文件特征包括文件中预设扇区数据对应的第一哈希值；所述基于预设文件特征，对所述数据交互指令对应的目标文件特征进行验证，包括：

10 计算所述目标文件中预设扇区数据的第二哈希值；

若所述第二哈希值与所述第一哈希值一致，则判定所述目标文件特征符合所述预设文件特征；

若所述第二哈希值与所述第一哈希值不一致，则判定所述目标文件特征不符合所述预设文件特征。

15 在本实施例中，预设扇区数据为预先选定的扇区中的数据，例如预设扇区为第一扇区，则计算计算机设备所要读写的目标文件所在的第一扇区部分数据的第二哈希值。在第二哈希值与第一哈希值一致时，则判定所述目标文件特征符合所述预设文件特征。示例性地，文件 A 中预设扇区数据 B 的第一哈希值为 533c3057ec5801aa39e9257066890928，当需要读写文件 A 中的预设扇区数据 B 时，计算读写到的文件 A 中的扇区数据的第二哈希值，并判断第二哈希值是否为 533c3057ec5801aa39e9257066890928，若是，则说明读写的是文件 A 中的预设扇区数据 B，符合预设文件特征，若否，则说明读写的不是文件 A 中的预设扇区数据 B，不符合预设文件特征。本实施例通过哈希值对比方式验证文件特征，能够更加精准的对某些文件数据进行读取控制。

25 在一些实施例中，所述对所述数据交互指令对应的目标文件特征进行验证之后，还包括：若所述目标文件特征不符合所述预设文件特征，则对所述目标文件进行隐藏。

在本实施例中，隐藏文件是指使计算机设备识别到文件。隐藏目标文件的方式可以是在返回数据包过程中通过修改目标文件的真实扇区地址（包括起始扇区地址、簇（块）链数据等）和文件大小，以使计算机设备将其识别为文件大小为 0 字节的空文件，而无法直接读取到目标文件的内容数据；也可以是在返回数据包过程中通过空白数据等非真实数据替代目标文件中的内容数据；还可以将目标文件修改为删除状态，以使计算机设备将其识别为文件已删除，而不显示该文件。可以理解的是，本实施例的替代或修改仅为伪装，并非对数据进行真实修改，而仅仅是对展示给计算机设备的数据进行替代或修改。

- 10 需要说明的是，在计算机设备与存储设备建立通信后，计算机设备需要读取存储设备的文件数据，以在计算设备上展示，则本实施例在计算机设备展示前，通过识别文件的预设文件特征，以对文件进行隐藏，其能够兼容本申请的所有保护模式，即在所有保护模式均可以隐藏文件，以使所有保护模式在隐藏文件后的存储设备进行权限配置，从而只对存储设备中未隐藏的文件进行读写，进而保护存储设备的隐私数据的安全性。

在一些实施例中，若保护模式为加密写入模式，所述步骤 S601，包括：

响应于所述数据交互指令，对所述数据交互指令携带的待写入数据进行加密处理，得到第一目标数据；

向所述存储设备中的所述目标文件写入所述第一目标数据。

- 20 在本实施例中，保护模块存储有用于数据加密的密钥。对于计算机设备需要在存储设备写入数据的场景，计算机设备发送携带有待写入数据的写入指令，通过保护模块对待写入数据进行加密处理，得到第二目标数据，再向存储设备写入该第二目标数据。

- 25 可选地，对于目标设备为中间设备时，中间设备响应于写入指令，并通过保护模块对待写入数据进行加密，得到第二目标数据，再将第二目标数据和写入指令转发至存储设备，由存储设备根据写入指令写入该第二目标数据。对于目标设备为具有保护模块的存储设备时，保护模块在数据写入前验证用

户身份（应理解，在其他实施例中也可以不用验证），如用户输入保护模块的解锁密码，以使保护模块能够在写操作时调用其预存的加密密钥，当存储设备接收到写入指令时，存储设备响应于写入指令，并通过保护模块对待写入数据进行加密，得到第二目标数据，对第二目标数据进行写操作。

- 5 需要说明的是，本实施例通过保护模块对待写入数据进行加密，以能够独立保护存储设备的数据安全，同时将加密密钥存储于保护模块，以实现密钥和数据分离保管。即使在存储设备丢失后，数据难以被破解，进一步提高数据安全性。

10 在一些实施例中，若保护模式为解密读取模式，所述响应于所述数据交互指令，对所述存储设备进行读操作和/或写操作，包括：

响应于所述数据交互指令，向所述计算机设备反馈第二目标数据，所述第二目标数据为对所述存储设备响应于所述数据交互指令返回的数据进行解密后的数据。

15 在本实施例中，保护模块存储有助于数据解密的密钥。对于计算机设备需要读取存储设备中的数据的场景，计算机设备发送读取指令，根据该读取指令获取存储设备中的目标数据，并通过保护模块对该目标数据进行解密处理，得到第三目标数据。

可见，本申请实施例提供的技术方案还可通过加密写入或解密读出，实现存储设备特定扇区地址数据的加密或解密。

20 具体实现方法：

1、对特定扇区地址的数据进行加密或解密，类似扇区限位读写模式的流程，预先配置(手动或自动)需要加密或解密的特定扇区区间集合。

2、当计算机发送的数据交互指令的读或写操作符合特定的加解密扇区区间，保护模块进行加密或解密：1) 如果是读取到特定加密扇区区间的数据时，
25 保护模块读取到存储设备的数据后，进行解密并向计算机响应；2) 如果是写入到特定加密扇区区间的数据时，保护模块将计算机写入的数据进行加密，再向存储设备写入。

具体应用场景：

1、手动配置加密扇区区间。例如，配置0~9999扇区区间为加密扇区区间。当读取到该扇区区间时，保护模块进行解密响应；当写入到该扇区区间时，保护模块进行加密写入。

5 2、计算机设备读写过程中的自动加密解密。例如，预先配置需要进行加密或解密的文件类型，保护模块再预先读取需要加密或解密的特定文件数据的首扇区地址及扇区地址集合。

3、保护模块的预先自动加密，计算机读写过程中自动加密解密。例如由保护模块自动加密引导扇区。类似扇区限位读写模式的流程，保护模块根据
10 存储设备引导扇区和文件系统的协议或规则，预先读取存储设备的MBR、GPT等引导扇区、文件系统引导扇区、文件分配表的扇区地址集合或扇区地址区间集合，并读取数据进行加密，并将加密数据按照原扇区地址进行写入，使存储设备存储的是加密后的引导扇区、文件系统相关的数据。

4、保护模块结合对特定文件读写过程的加解密。例如，对指定读写的特定文件夹内的文件读写操作进行加解密，比如将test.txt文件写入至safedir文件
15 夹内自动进行加密，读出自动解密。其他文件夹不进行加密或解密操作。对指定读写的特定文件类型进行加解密，例如对txt文件类型进行加解密控制，当test.txt文件写入时，自动进行加密，读出时进行解密。

这样做的优点：加密或解密的密钥数据存储在保护模块中，也由保护模块
20 块执行加密或解密的操作。一是,保护模块与存储设备可以在物理上分离保管，当存储设备丢失时，无法被恶意逆向获取密钥数据（现有技术，将密钥与存储设备为物理一体化设计容易被逆向提取密钥数据，例如带有加密功能的 U 盘）；二是，密钥不经过计算机加密或解密，计算机无法获得密钥数据，防止计算机被恶意控制后，密钥被窃取（现有技术，将密钥存储在计算机中，
25 由计算机执行加密或解密的操作，例如加密 U 盘，需要在计算机安装 U 盘的加密或解密软件）；三是，具体的加密扇区地址区间，只有保护模块知晓，计算机直接通过存储设备读取难以分析，从而难以发现加密数据的存在。四

是，加解密过程无需计算机设备参与，计算机无法获知或控制加解密的过程。

可选地，对于目标设备为中间设备时，计算机设备发送读取指令，中间设备将读取指令转发至存储设备，存储设备根据该读取指令获取目标数据，并转发至中间设备，中间设备的保护模块对该目标数据进行解密，得到第三目标数据，并将第三目标数据转发至计算机设备。对于目标设备为具有保护模块的存储设备时，保护模块在数据读取前验证用户身份（应理解，在其他实施例中也可以不用验证），如用户输入保护模块的解锁密码，以使保护模块能够在读操作时调用其预存的解密密钥；在计算机设备发送读取指令后，存储设备根据该读取指令获取目标数据，并通过保护模块对该目标数据进行解密处理，得到第三目标数据，再将第三目标数据返回至计算机设备。

需要说明的是，本实施例通过保护模块对存储设备获取到的数据进行解密，以能够独立保护存储设备的数据安全，同时将解密密钥存储于保护模块，以实现密钥和数据分离保管。即使在存储设备丢失后，数据难以被破解，进一步提高数据安全性。

可以理解的是，解密读取模式和加密写入模式能够兼容其他保护模式，例如当前保护模式可以同时为特定文件读写模式、解密读取模式和加密写入模式。

在一些实施例中，若所述保护模式为人工确认模式，所述步骤 S601，包括：

20 响应于所述数据交互指令，提示用户是否确认执行所述数据交互指令；

若接收到所述数据交互指令的确认执行指令，则继续对所述存储设备中的目标文件进行读写操作。

基于预设的规则，对计算机发送的数据交互指令，例如读、写特定扇区地址进行人工确认，如果确认就继续在存储设备中执行数据交互指令，如果不确认则不执行。

具体实现方法：

基于预设的数据交互指令的规则，保护模块判断该交互指令是否需要进

行人工确认。

预设的数据交互指令的规则可以有但不限于：

1、基于扇区地址读写操作时的人工确认。例如：一是类似扇区限位读写模式的流程，建立存储设备引导区、文件系统引导区的扇区区间集合，或者
5 建立特定文件数据的扇区区间集合。作为需要人工确认的扇区区间。

2、基于文件属性操作时的人工确认。例如：类似文件限制读写模式的流程，一是建立针对特定文件类型（根据文件后缀、文件内容数据特征等）的创建、删除、修改文件属性，以及读写文件内容数据的规则；二是建立针对
10 不特定文件的创建文件、修改文件属性、删除文件的规则。例如，设置exe可执行程序读写需要确认时，当计算机读出或写入存储设备的文件名为abc.exe的文件时，中间设备或者保护模块监听到这个动作，不马上进行响应，而是通过亮灯、或者屏幕显示的方式，要求人工对此操作进行确认。经过人工确认后，中间设备或保护模块才会进行响应，继续文件的读写操作。

3、基于设备接入操作时的人工确认。例如，保护模块发现计算机设备开始连接枚举存储设备了（读取设备描述符、配置描述符、接口描述符、端点
15 描述符、字符串描述符、设备容量信息等等），进行人工确认连接。保护模块发现计算机设备发送特定的指令（例如带有标记、密码、密钥的描述符请求），在人工确认符合约定后，再进行人工确认连接。

这样做的优点：存储设备用户可以知晓数据或具体文件的写入或读出的
20 传输过程，进一步对存储设备内的扇区数据或具体文件传输具有的精细化控制权（现有技术无法实现，仅能够通过只读控制）；防止计算机设备对存储设备进行用户不知晓的操作，例如恶意格式化存储设备，或者盗取复制敏感文件，或者恶意修改敏感文件，或者写入恶意程序文件等。同时，让计算机设备用户显性的知晓文件数据传输的内容，可以无需通过计算机软件进行控制
25 或杀毒软件的方式，避免计算机或计算机控制软件、杀毒软件的不可靠性。

在本实施例中，人工确认模式为在数据交互过程需要用户参与确认的模式。即针对计算机设备发送的数据交互指令，需要人工方式在中间设备或者

带有保护模块的存储设备上确认。例如，对于 exe 可执行程序，计算机设备需要读写存储设备中的 abc.exe 文件时，保护模块监听到该读写操作时，通过亮灯或者屏幕显示等方式，提示用户对此该读写操作进行确认。经过人工确认后，再执行对应的读写操作。可以理解的是，人工确认模式能够与其他

5 保护模式兼容。

示例性地，目标设备以中间设备为例，如图 12 所示的中间设备的示意图，当计算机设备需要向存储设备中的 abc.exe 文件写入数据时，中间设备显示对应操作信息，当用户点击确认选项时，表示触发确认执行指令，则允许计算机设备向存储设备中的 abc.exe 文件写入数据，当点击取消选项时，则中断该

10 操作。

需要说明的是，本实施例通过人工确认模式能够对一些场景下的非法行为进行监控，以避免计算机设备在用户不知情时非法读写存储设备而造成数据泄露或者安全隐患，从而提高存储设备和计算机设备的安全性。

也就是说：当前保护模式是人工确认模式时，上文中提及的“所述数据交互指令针对的数据源是所述当前保护模式指定的至少一个数据源中的一个，且所述数据交互指令对所述数据源内数据的操作类型符合所述当前保护模式规定的操作类型时，对所述数据交互指令做出响应”，可具体为：

15

所述数据交互指令针对的数据源是人工确认模式指定的至少一个数据源中的一个，且所述数据交互指令对所述数据源内的操作类型为读写类型时，

20 显示预写入或读出数据的相关信息；

响应于用户针对所述相关信息触发确认操作，基于所述数据交互指令向存储设备写入或读取所述数据。

本文中提及的只读模式可包括但不限于全盘只读模式、部分盘只读模式等等。下面的实施例中将以全盘只读模式为例，即在一些实施例中，若所述

25 保护模式为全盘只读模式，所述步骤 S601，包括：

响应于所述数据交互指令，向所述计算机设备反馈第三目标数据，所述数据交互指令为读取指令，所述第一目标数据为所述存储设备响应于所述读

取指令返回的数据。

在本实施例中，全盘只读模式为允许计算机设备读取存储设备中的所有文件数据的模式。计算机设备在希望与存储设备进行数据交互时会发送数据交互指令，但在全盘只读模式下，只有读取指令满足权限要求，目标设备也只会响应读取指令，并向计算机设备反馈第一目标数据，第一目标数据为从存储设备中读取到的数据。

示例性地，目标设备对数据交互指令的指令类型进行识别，并根据读写权限进行验证，在全盘只读模式下，当数据交互指令为读取指令时，目标设备根据读取指令调取存储设备中的第一目标数据，并将第一目标数据发送至计算机设备。当数据交互指令不为读取指令时，例如写入指令（如 SCSI 协议的指令 2A，代表写）或其他类型的指令时，则该数据交互指令不会转发至目标设备。可选地，对于数据交互指令不为读取指令的情况，保护模块不转发数据交互指令，并且会向计算机发送已执行完毕的反馈信息，实现对计算机读写权限的限制。

本实施例通过全盘只读模式对存储设备与计算机设备之间的数据交互进行控制，以避免计算机设备对存储设备的数据进行修改或删除，从而保护存储设备的数据安全性。

在一些实施例中，在一些实施例中，在图 1 所示实施例的基础上，图 12 示出了第四实施例提供的数据安全保护方法的流程示意图。与图 1 相同的步骤不再赘述，如图 12 所示，针对读写操作的执行过程，所述方法还包括：

步骤 S701，基于预设读写规则，对所述读写操作进行异常验证；

步骤 S702，若所述读写操作不符合所述预设读写规则，则判定所述读写操作异常。

基于预设规则，对计算机发送的数据交互指令（例如读或写扇区地址）进行自动验证，如果不符合规则，不执行，或者进入人工确认模式判断。

具体实现方法主要建立规则，规则主要有但不限于：

1、基于计算机正常枚举，读写文件系统的规则。例如，计算机读写的规

则是：先读取 0 扇区地址（分析引导扇区数据，读取文件系统引导扇区地址）
—>读取文件系统引导扇区地址（分析文件系统的文件分配表和首目录扇区地址）
—>读取文件分配表扇区地址数据—>读取首目录扇区地址数据。

- 5 以上的规则是有规律和跳跃式的，从 0 扇区地址开始，是非连续式的，一般为跳转的。如果恶意读取，分析读取时，则直接从扇区至特定扇区区间地址连续读取，且没有计算机正常读写文件系统的规律，则认为是异常。

- 2、基于计算机正常读写文件的上下文规则。例如计算机在读取文件内容数据时，会有先读取其文件所在的文件夹数据的记录（获取文件开始扇区地址（或称首簇、首块等））；写入文件数据时，会有先写入文件所在的文件夹数据的记录（记录文件开始扇区地址（或称首簇、首块等））。如果没有
10 该上下文操作则认为是异常。

- 3、基于文件系统数据管理的规则。例如文件系统一般将多个扇区地址划分为一个扇区区间进行管理（FAT 文件系统“簇”，或者其他文件系统“块”）。计算机正常操作文件系统时，应该是从该簇或块的首扇区地址开始
15 执行读或写的操作。如果没有从簇或块的首扇区地址开始操作读或写，操作的扇区地址为簇的其他位置，则认为是异常。

- 4、基于业务习惯的规则。例如计算机在预设的时间内（或者一次接入内）向存储设备读取了多个文件（超过预设数量），则认为是异常。

根据异常做出相应处理可包括但不限于：

- 20 禁止操作时，保护模块可以返回执行成功的响应、或者响应空白数据、或者响应其他非真实的数据，使计算机认为执行成功，实际上保护模块没有真正的操作存储设备的数据，防止计算机认为操作失败，不断尝试操作。二是转入人工确认模式的流程。

- 在本实施例中，预设读写规则包括但不限于扇区地址的通用读写规则和
25 文件读写数量等。示例性地，对于扇区地址的通用读写规则，通常从首扇区地址开始读写，若当前读写操作未从文件的首扇区地址开始读写，而是在其他扇区开始读写，如在数据区的第 100 扇区连续读写至 9999 扇区，则认为读

写操作异常行为。对于文件读写数量，由于爬虫式读取是对存储设备的所有文件进行扫描并批量读取，所以通过设置文件的读取数量，例如 10 个，若超过 10 个则认为读写操作异常。

进一步的，本实施例提供的方法中步骤“对所述数据交互指令做出响应”

5 可包括：

步骤 41、将所述数据交互指令发送至存储设备，以便存储设备基于所述数据交互指令读取数据和/或写入数据；

步骤 42、获取所述存储设备基于所述数据交互指令读取数据和/或写入数据的过程信息；

10 步骤 43、基于过程信息，确定是否存在异常；

步骤 44、若存在异常，则向存储设备发送停止指令。

基于上文中提及的有关计算机设备正常读取文件的规则中的相应内容，上述步骤 43“基于过程信息，确定是否存在异常”，可包括如下中的至少一项：

若所述存储设备基于所述数据交互指令读取数据的过程不符合设定过程
15 规律，则确定存在异常；

若所述存储设备基于所述数据交互指令读取数据和/或写入数据的过程没有指定上下文操作，则确定存在异常；其中，读取数据时，指定上下文操作为读取该数据所在文件夹的操作；写入数据时，指定上下文操作为获取所述数据所在文件夹的操作；

20 若所述存储设备基于所述数据交互指令读取数据和/或写入数据的过程没有从所述数据所在簇或块的扇区首地址开始读或写操作，则确定存在异常；

若所述存储设备基于所述数据交互指令在预设时长内读取了超过设定数量个文件，则确定存在异常。

可选地，读写操作异常时可以结合人工确认模式进行人工确认，或是向
25 计算机设备反馈信息。例如，本申请实施例提供的方法还可包括如下步骤：

步骤 51、若存在异常，则向计算机设备发送反馈信息；其中，所述反馈信息包括：模拟写入成功的虚假信息，或将预设数据作为成功从存储设备读

取的数据；和/或

步骤 52、若存在异常，则输出人工确认提示信息，以便用户基于所述人工确认提示信息确定是否继续执行。

在一些实施例中，在图 1 所示实施例的基础上，图 13 示出了第五实施例提供的数据安全保护方法的流程示意图。与图 1 相同的步骤不再赘述，如图 13 所示，所述方法还包括：

步骤 S801，将目标扇区区间作为存储数据源接入到所述计算机设备，所述目标扇区区间通过切割所述存储设备的存储空间得到，所述存储数据源包含所述目标文件。

10 在本实施例中，保护模式为逻辑分盘模式时，对存储设备进行逻辑分盘，逻辑分盘为基于存储设备的扇区地址对存储设备进行存储空间切割的过程，其区别于当前仅在计算机设备上显示多个分区而实际上文件存储于同一个扇区区间的系统磁盘分区。例如，将硬盘 1 的扇区地址区间为 0-999，对硬盘 1 进行系统磁盘分区，以在计算机设备上显示盘 1 和盘 2，但盘 1 和盘 2 的数据
15 实际上还是存储于硬盘 1 中 0-999 扇区地址区间，也可以同时访问盘 1 或盘 2 的数据。而本实施例的逻辑分盘模式是将硬盘 1 的扇区地址区间分为 0-499 和 500-999 两个扇区地址区间，并分别对应 A 盘和 B 盘，则 A 盘的数据存储于 0-499 的扇区地址区间，B 盘的数据存储于 500-999 的扇区地址区间，从而使 A 盘数据和 B 盘数据在底层逻辑上也互不影响，例如可以分别格式化为不同的
20 文件系统。可选地，对于切割后的多个扇区区间，可以独立分盘形式接入到计算机设备，也可以文件形式接入到计算机设备。

即当前保护模式为逻辑分盘模式时，相应的，本申请实施例提供的所述方法还可包括如下步骤：

步骤 61、若用户选出的当前保护模式为逻辑分盘模式，则对所述存储设备的特定存储空间进行划分，得到至少一个分盘；
25 步骤 62、从所述至少一个分盘中选定一个分盘作为目标分盘，接入所述计算机设备。

进一步的，本申请实施例提供的所述方法还可包括如下步骤中的至少一个：

步骤 a、响应于用户的设置，确定所述特定存储空间；所述特定存储空间可以是存储设备的全部或部分空间；

5 步骤 b、基于所述逻辑分盘模式中特定存储空间的选定规则，确定所述特定存储空间。

其中，上述步骤 61 中“对所述存储设备进行分盘操作，得到至少一个分盘”，可包括：

响应于用户的划分指令，读取所述特定存储空间的扇区信息，基于所述
10 扇区信息，对所述特定存储空间进行划分；或者

读取所述特定存储空间的扇区信息，基于所述扇区信息并利用预置的划分策略，对所述特定存储空间进行划分；或者

在存储设备的文件系统中，生成至少一个镜像文件，以所述至少一个镜像文件分别对应的地址区间，对所述存储设备的特定存储空间进行划分。

15 具体的，“预置分盘策略”可在本地获取所述预置分盘策略；或者从网络侧服务端，获取所述预置分盘策略。

需要说明的是，本申请中的服务端为使用网络连接（如使用 TCP/IP 等连接）或非网络连接（如使用蓝牙、LoRA 等的点对点连接）的终端。举个例子来说，两个终端建立数据交互关系，第一终端向第二终端提供了可供读写操作的数据源，那么第一终端即可理解为是服务端。当然，服务端还可以理解为如部署在网络侧服务器、虚拟服务器、云端、服务器集群等等。另外，本申请的扇区应理解为广义上的存储空间地址，即为对存储设备的存储空间进行划分的区域，扇区信息包括但不限于扇区总数（扇区地址区间）和各扇区字节数等。逻辑分盘模式能够兼容所有保护模式，即其他保护模式针对的是
20 在逻辑分盘后接入到计算机设备的目标分盘，对于未接入到计算机设备的其他分盘，计算机设备无法识别到其他分盘，所以计算机设备所发送的数据交互指令只能面向目标分盘。
25

通过逻辑分盘模式，实现效果类似于计算机的“电脑双硬盘双系统”，通过两个硬盘物理隔离卡切换硬盘选择内网系统或外网系统，存储区与系统之间各自独立。这里的分盘，是将只有 1 个物理存储区、或逻辑上为 1 个物理存储区的存储设备进行划分，在逻辑划分成任意数量和容量大小的 2 个以上的

5 存储区。

具体实现方法：

1、预先划分分盘，并选定分盘。预先在存储设备中划分多个扇区区间，并选择对应的扇区区间。例如存储设备的可用总扇区为 2000 个，平均分为 2 个分盘，每个盘可用扇区总数为 1000 个。此外，可以对每个分盘自动分配、

10 或手动分配：厂商 ID（Vendor ID）、设备 ID（Product ID）、字符串信息等硬件特征参数。

2、响应计算机请求硬件特征参数。一是响应分盘容量参数。当计算机设备在发送请求容量参数的指令时，响应选定分盘的容量的相关总数。例如，当计算机发送 SCSI 或 UFI 指令代码为：0x25（READ CAPACITY）时，保护

15 模块响应该逻辑分盘的最后逻辑块地址。当计算机发送 SCSI 或 UFI 指令代码为：0x23（SCSI_READ_FORMAT_CAPACITIES）时，保护模块响应可用的扇区（或者称可用块）的数量以及单个扇区（或者块）的字节数。从而使计算机认为存储设备的容量值为逻辑分盘的容量值。二是响应分盘的厂商 ID（Vendor ID）、设备 ID（Product ID）等硬件特征参数。当计算机发送请求

20 硬件特征参数的指令时，响应分盘对应的硬件特征参数。例如，当计算机发送 USB 协议中的设备描述符（0x80 0x06 0x00 0x01 0x00 0x00 0x12 0x00）请求时，保护模块在设备描述符中，响应对应的厂商 ID（Vendor ID）、产品 ID 参数。三是响应分盘的字符串信息参数。当计算机发送请求字符串描述符的指令时，响应分盘对应的字符串信息。例如，当计算机发送 USB 协议中的字

25 符 串 描 述 符 的 （ 0x8006010309040200 、 0x8006020309041200 、 0x8006030309042800）请求时，保护模块在字符串描述符中，响应对应的字符串信息。

- 3、读写映射。当计算机发送数据交互指令时，保护模块偏移映射到对应的扇区区间。当选择盘 1 时，计算机读取 0 扇区，则读取移动存储设备的 0 扇区并返回；计算机读取 1 扇区，则读取存储设备的 1 扇区并返回，依此类推，最大可读为扇区 999；当选择盘 2 时，计算机读取 0 扇区，则偏移 1000 扇区，读取移动存储设备 1000 扇区并返回；计算机读取 1 扇区，则读取存储设备的 1001 扇区并返回，依此类推，最大可读为扇区 1999，无法读取存储设备 0-999 扇区数据。计算机写 0 扇区地址、1 扇区地址也与上述读的偏移映射的扇区位置一致，以此类推。当计算机读或写的扇区地址超出分盘的范围时，返回读或写错误的状态。
- 10 如果存储设备的容量为 2000k 字节，假设该存储设备分盘后有两个分盘，分别为分盘 1 和分盘 2。分盘 1 和分盘 2 的容量相同，比如均为 1000k 字节。在选择盘 2 时，计算机显示的总容量则为 1000k 字节。将盘 2 进行格式化和数据拷贝等操作，不影响分盘 1 的所有数据。这里需要补充的是：以上扇区区间、总容量数据举例是为了便于理解，实际场景下数量会大得多。
- 15 逻辑分盘与特定文件夹读写的不同。逻辑分盘实现思路与特定文件读写、空白文件夹大致一致，主要是将计算机读写交互指令的扇区地址映射到存储设备的相关扇区地址。特定文件夹读写、空白文件夹主要是将一个文件的扇区地址映射到另外一个文件的扇区地址，文件系统、存储的总容量与剩余空间与原盘一致，文件系统不能被格式化。分盘模式则是不考虑具体的文件，
- 20 直接对一段扇区地址区间进行映射，存储的总容量与剩余空间为各自独立的，文件系统可以各自格式化。

存储设备分盘的具体场景：

- 一是自动进行外部存储的划分逻辑分盘（存储介质分盘）。作为中间设备或读卡器的形式，对任意接入的存储设备进行分盘。保护模块预先读取存储设备（接入的 U 盘、SD 卡、TF 卡）的基本信息：扇区总数、各个扇区字节数、厂商与设备 ID、字符串信息等。例如，当存储设备（例如 U 盘等）容量为 16G，如果默认将存储设备平均为 2 个分盘，则自动分为 2 个 8G 的分盘

盘；如果默认将存储设备分成 3 个分盘，分为 1 个 8G 的分盘，2 个 4G 的分盘，32G 则为 16G 和 2*8G，64G 则为 32G 和 2*16G 等等。

二是自动进行内部存储空间的划分（存储介质分盘）。作为集成在移动存储设备的形式，可内部存储（FLASH）一个或者多个物理存储区进行逻辑上的分盘。由于存储介质固定在设备内部，存储物理容量是出产时就已知且固定的，所以免去上述预先读取存储设备的基本信息的步骤。预设好存储介质设备的基本信息：扇区总数、各个扇区字节数、厂商 ID 与设备 ID、字符串描述符等。

三是通过文件镜像形式进行分盘。在存储介质的文件系统中，生成镜像文件，以镜像文件的内容数据作为分盘的扇区区间进行分盘。将分盘的所有扇区直接映射到某个特定文件的内容数据内。分盘的大小可以通过文件占位的方式进行预先设置，例如生成 16G 大小的空白“分盘 1.dd”文件，这时候分盘大小为 16G；也可以不通过预先占位，而是在有读写需要时，通过在文件数据追加的方式写入，这时候分盘大小为分盘已有数据的大小加上 U 盘的总剩余空间（或者叫空白数据区域），能够充分利用存储设备的数据空间。进一步具体的，例如分盘镜像文件路径为“我的 U 盘\我的文件夹\分盘 1.dd”。并预设分盘对应的基本信息（扇区总数、各个扇区字节数、厂商 ID 与设备 ID、字符串信息等）。

在使用该分盘 1 时，在计算机枚举时，保护模块返回分盘的基本信息，计算机在读写数据时，保护模块实际读写“分盘 1.dd”的文件内容数据进行映射。例如计算机读取 0 扇区时，则返回“分盘 1.dd”文件内容数据的首扇区地址；计算机读取 100 扇区地址数据时，则返回“分盘 1.dd”文件的 100 扇区地址数据；计算机将数据写入 200-300 扇区时，则将数据写入“分盘 1.dd”文件的 200-300 扇区地址数据。

四是通过网络服务的方式进行分盘（实际上为联网数据源接入了）。同文件镜像形式进行分盘的原理，在存储设备本地或服务端预设好分盘对应的基本信息：扇区总数、各个扇区字节数、厂商 ID 和设备 ID、字符串信息等。

不同之处是生成和使用的镜像文件存储在服务端中。联网保护模块（联网 U 盘）本身可以不存储数据、或者存储少量数据（用于优化启动方式，或者连接网络服务端的网络配置），联网 U 盘通过有线或无线等方式，连接网络服务器，并发送联网 U 盘的标识信息。后台服务器根据联网 U 盘的标识信息关联对应的镜像文件（如“分盘 1.dd”）。在计算机在向 U 盘发送交互指令时（例如读取扇区），向服务器转发交互指令的读写要求（命令主要信息为：读或写操作，开始的扇区地址，连续读或写扇区的长度）。服务器接到 U 盘的发送的请求后，返回关联对应的镜像文件（如“分盘 1.dd”对应盘 A）文件对应的扇区地址数据。此外，标识号可以绑定“分盘 1.dd”对应盘 A、“分盘 2.dd”对应盘 B、“分盘 3.dd 对应盘 C”3 个文件，可以根据进行数据源的切换。

另外，对于上述逻辑分盘模式（对接入存储设备（如 U 盘）进行划分、内部存储介质划分、以文件进行存储的镜像文件划分、网络镜像文件划分）都需要能够自定义描述符的参数，以让计算机能够区分为不同的存储设备（例如不同的 U 盘），实现的方式为“配置信息”+“数据源”。配置信息包括：描述符集合和基本信息。描述符集合包括：设备描述符、配置描述符、接口描述符、端点描述符等，基本信息包括：扇区总数、各个扇区字节数等容量信息，只读或可读写状态等大容量存储设备的参数。此外，“配置信息”可以存储在数据源的隐藏位置，例如最后一个扇区并不能被计算机当作 U 盘数据访问；也可以在服务端的数据库中存储；也可以是保护模块内置存储的某个扇区或者文件进行存储等等。

这样做的优点是：

可以充分发挥存储设备的存储空间，相比使用多个存储设备或存储芯片进行切换以实现隔离的方式有效减低了硬件成本，做到一个存储设备或存储芯片满足多种不同的需求，例如可以在分盘模式中格式化不同的文件系统，实现不同场景的使用。另外，可实现更安全的保护，各个分盘直接相互独立（数据源独立，硬件特征也可以不同），在数据通信层进行控制，计算机仅认为接入的存储设备为分盘的容量，不会超范围进行扇区读取。如果强行超

分盘范围扇区读取，保护模块也不会执行该指令。还有，本申请实施例提供的方案，可以不依赖存储设备的类型、种类和所格式化的文件系统，只要能与保护模块建立通信连接和读写控制，就能实现逻辑分盘。

数据存储在服务端中，保护模块可以根据不同的场景随时切换数据源。

- 5 数据读取和写入都保存在服务端中，保护模块本质上只是一个前端设备。当保护模块丢失后，数据还保存在服务端中。此外，计算机设备无法获知数据源，保护模块可以不通过计算机的网络联网，使用自带的移动蜂窝网络，或保护模块用户的 wifi 等，网络流量不经过计算机。还有，对于计算机来说，无法直观的管制存储设备的数据是存在服务端，还是在保护模块本地的存储
- 10 介质中。另外，本申请实施例的保护模块不同于现有网络 U 盘，现有技术是先将服务端的文件下载的网络 U 盘存储设备中，再通过计算机读取存储设备的文件系统的文件进行下载；或者计算机先将文件写入到 U 盘的存储设备的文件系统中，再由网络 U 盘上传到服务端。这样的话，需要占用网络 U 盘自身存储空间的容量，例如 16G 的网络 U 盘无法传输 32G 的文件，或者剩余空
- 15 间不足 4G 的网络 U 盘，无法传输大于 4G 的文件。本发明通过数据转发，不存在文件限制的问题。另一方面，无法对整个存储分盘的数据进行切换。而在本发明基于扇区地址的读写，盘 A 对应可以格式化为 FAT32 文件系统，文件有 A.txt、B.txt；盘 B 可以格式化为 ExFAT 文件系统，文件有 C.txt、D.txt，并可以直接接入计算机进行显示。而现有的网络 U 盘只能选择特定的文件进
- 20 行拷贝。另外，服务端的映射的“分盘 1.dd”等镜像文件，在基于分布式存储技术、优化存储和 CDN 网络加速的情况下，可以为数据库的数据，或者多个文件的组合、拼接、映射等等。

选择数据源的方式：

- 1、物理按钮选择，通过保护模块物理按钮切换（如图 2b 和 2c 中的对应
- 25 分盘数据源选择的物理切换按钮），选择对应的分盘数据源（如存储介质分盘、镜像文件分盘、联网镜像文件分盘等）。

2、近场通信选择。通过保护模块的蓝牙、wifi、串口接口等通信模块，

向其发送选择分盘数据源的指令。保护模块收到指令后，选择对应的分盘数据源。

3、远程通信选择。通过保护模块联网的方式，在服务端获取分盘数据源的指令，并选择对应的分盘数据源。服务端的指令由用户通过 APP、小程序、

5 网页等程序连接服务端进行设置。

4、由计算机发送的密钥（或特征值）进行选择。分盘在切割创建时，其基本信息中带有对应的密钥信息。保护模块在接入到计算机后，计算机发送带有密钥（或特征值）信息的交互指令，保护模块根据密钥匹配分盘基本信息集合。当匹配命中时，选择对应的分盘数据源，例如，分盘 1 对应密钥 A，
10 分盘 2 对应密钥 B，同时接入所有分盘的密钥为 C，当验证指令携带密钥 A 时，确认将分盘 1 接入到计算机设备；当验证指令携带密钥 B 时，确认将分盘 2 接入到计算机设备；当验证指令携带密钥 C 时，确认将分盘 1 和分盘 2 同时接入到计算机设备。在接入计算机设备时，通过计算机发送的密钥进行验证，以确定接入选中的目标存储数据源，从而提高存储数据源的安全性。

15 基于上述选择数据源的方式可知，本申请实施例提供的所述方法中步骤“从所述至少一个分盘中选定一个分盘作为目标分盘”可包括：

响应于用户通过交互装置对所述至少一个分盘的选择操作，将用户选定的一个分盘作为目标分盘；或者

20 接收到指定设备发送的分盘选择指令时，将所述分盘选择指令指示的分盘作为目标分盘；其中，指定设备通过近场通信或远程通信方式与保护模块通信；

其中，所述指定设备与所述计算机设备为不同的设备；或者

接收计算机设备发送的携带有盘密钥的信息，对所述盘密钥进行验证，验证通过后，将所述至少一个分盘中具有该盘密钥的分盘作为目标分盘。

25 可选地，目标分盘的接入方式可以为通过拨动开关、远程遥控、计算机配置的方式进行设置。示例性地，在一种可能实施的方式种，目标设备设置有用选分盘的物理开关，通过拨动物理开关以选中目标分盘。在另一种

可能实施的方式中，目标设备设置有如无线局域网、蓝牙、红外线或超宽带的通信单元，以用于与远程遥控设备进行连接，从而通过远程遥控设备选中目标分盘。在又一种可能实施的方式中，通过计算机设备通信连接，以通过该计算机设备选中目标分盘。

- 5 可选地，计算机设备读取存储设备的总扇区数时，向计算机设备返回选中分盘的扇区总数；计算机设备发送读写扇区的数据交互指令时，按照分盘扇区的真实扇区位置进行映射。

- 10 这里需要补充的是：上文中提及的“目标扇区区间通过切割存储设备的存储空间”中的“切割”，以及上文中提及的“对存储设备的特定存储空间进行划分”中的“划分”，在实际的技术本质上可以理解为是一种映射策略。该映射策略可预先配置好。对于存储介质（或存储设备）来说实际上没有任何的改变，其磁盘容量信息、扇区地址读写没有变化；只是在保护模块中基于这个映射策略，使得使用者在计算机设备侧看到的是分盘的效果。换句话说，保护模块对存储介质的特定存储空间的划分，是虚拟的、概念上的分盘划分，在计算机设备侧呈现给用户的是分盘效果，存储介质上没有任何变化。

在一些实施例中，在图 13 所示实施例的基础上，步骤 S801 之前还包括：

读取所述存储设备的扇区信息；

基于所述扇区信息，切割所述存储设备的存储空间，得到所述存储设备对应的多个扇区区间，所述目标扇区区间为多个所述扇区区间中的至少一个。

- 20 在本实施例中，基于预设分盘数量，对所述存储设备的扇区地址区间进行切割，得到每个存储空间的扇区地址区间。预设分盘数量可以为预设值，也可以在逻辑分盘前用户实时选择的数量。区间划分方式可以为基于预设区间大小对存储设备进行扇区地址划分的方式，也可以为基于用户实时选择的区间大小对存储设备进行扇区地址划分的方式。

- 25 可选地，若预设分配数量为预设值，当计算机设备与存储设备通信连接后，当目标设备在逻辑分盘模式下，按照默认值对存储设备的扇区信息进行区间划分，以实现即插即用。

示例性地，若预设分配数量为实时选择的数量，当计算机设备与存储设备通信连接后，当目标设备在逻辑分盘模式下，在计算机设备上显示用于提供用户选择分盘数量和各个分盘大小的选项，基于用户实时选择的分盘数量和分盘大小，对存储设备进行逻辑分盘。例如，存储设备的扇区地址区间为 0-1999，在计算机设备上显示分盘数量选项和分盘大小选项，如用户选择分盘数量为 2，每个分盘大小相同，则得到扇区地址区间 0-999 对应的分盘，以及扇区地址区间 1000-1999 对应的分盘。

可以理解的是，对于目标设备为中间设备时，中间设备同时接入多个存储设备，可以对多个存储设备进行逻辑分盘，也可以基于每个存储设备进行物理分盘，得到与存储设备数量相同的分盘数量。

图 14a、14c、14e 和 14g 示出了逻辑分盘模式对应的一个示例图。图 14a 示出存储介质（如具有保护模块的 U 盘或连接有中间设备的 U 盘）的可用空间显示值为 14.9GB（理论上可用空间约 16GB 左右）。图 14b 是从物理视角示出了对可用空间未进行逻辑分盘前的存储空间对应的示意图，如从 0x00 扇区位置至结束扇区位置间（即可用空间对应的扇区数或可用空间最后逻辑块地址+1）。假设要分为 1 个 8GB（理论值）的分盘、2 个 4GB（理论值）的分盘，共 3 个逻辑分盘。参见图 14c 示出了第 1 个逻辑分盘相关的信息，如容量、文件系统、分盘单元大小、备注等等，还可对格式化选项中的快速格式化进行勾选，还可通过“还原设备的默认值”控制触发还原默认值的操作，等等。如图 14c 所示的示例，显示有第 1 个逻辑分盘的容量 7.47GB（理论上可以是 8GB），文件系统为 FAT32(默认)，分配单元大小为 4096 字节等。图 14c 所示的窗口是在选择第 1 个逻辑分盘后显示出的格式化页面。该格式化页面中显示该第 1 个逻辑分盘的容量为 7.47GB（理论值 8G），用户点击“开始”控件后，便可对第 1 个逻辑分盘进行重新格式化。图 14d 是从物理视角示出了第 1 个分盘对应的 8GB 存储空间的示意图。参见图 14e 和 14g，显示了另第 2 个逻辑分盘的属性信息，即两个 4GB 的逻辑分盘，disk_02 和 disk_03。图 14f 是从物理视角示出了第 2 个分盘对应的 4GB 存储空间的示意图。图 14h

是从物理视角示出了第 3 个分盘对应的 4GB 存储空间的示意图。

经过分盘后，各盘对应的扇区区间相互独立，互不干扰，数据相互隔离。例如上述的 3 个逻辑分盘的文件目录完全不同，也无法互相访问。

图 14i 示出了在保护模块未进行逻辑分盘时特定文件夹模式下响应计算机读写存储空间的示意图。参见图 14i 所示，虚线指向的是计算机设备欲读/写根目录扇区数据，实际上保护模块在接收到计算机发送的读/写根目录扇区数据的数据交互指令后，保护模块读/写特定文件夹目录扇区数据并返回。

图 14j 示出了保护模块当前保护模式为逻辑分盘模式与空白文件夹模式的组合模式，并在逻辑分盘模式和空白文件夹模式的组合模式下将存储空间分出 3 个逻辑分盘的情况下响应计算机读写存储设备的示意图。如图 14j 所示，虚线指向的是计算机设备欲读/写根目录扇区数据，该根目录扇区位置可偏移至第 2 个逻辑分盘对应的扇区位置。计算机设备发送读/写根目录扇区数据的数据交互指令后，保护模块选择分盘 2，保护模块读/写分盘 2 上特定文件夹目录扇区数据并返回。

15 在一些实施例中，在图 1 所示实施例的基础上，图 15 示出了第六实施例提供的数据安全保护方法的流程示意图。与图 1 相同的步骤不再赘述，如图 15 所示，所述方法还包括：

步骤 S901，将镜像文件作为所述存储数据源接入到所述计算机设备，所述镜像文件基于预设镜像策略生成得到。

20 在本实施例中，预设镜像策略可以通过创建空白镜像文件的方式得到；也可以复制已有镜像文件的方式得到，还可以通过对所述存储设备的数据区间进行镜像的方式得到。

示例性地，对于创建空白镜像文件的方式：在存储设备上生成一个预设存储镜像文件（可以是 16G 大小的空白文件“分盘 1.dd”），得到镜像文件。
25 对于复制已有镜像文件的方式：将另一存储设备 A 硬盘的所有扇区区间的数据保存为“A 硬盘镜像文件.dd”的存储文件，则“A 硬盘镜像文件.dd”称为 A 硬盘的镜像文件，再将“A 硬盘镜像文件.dd”拷贝到具备存储空间能力的存储设

备中。通过保护模块，可以将上述“分盘 1.dd”或者“A 硬盘镜像文件.dd”作为数据源接入计算机设备。

可选地，对于对所述存储设备的数据区间进行镜像的方式，数据区间的大小可以通过文件占位的方式进行预先设置，例如生成 16G 大小的空白“分盘 1.dd”文件，则数据区间的大小为 16G；也可以在有读写需要时，通过文件数据追加的方式写入，则数据区间的大小为数据区间已有数据的大小加上存储设备的总剩余空间（或称空白数据区域），从而能够充分利用存储设备的数据空间。

示例地，计算机设备对以文件形式的存储数据源进行读写：数据区间对应的文件路径为 U 盘中的“E:\我的文件夹\分盘 1.dd”，当读写该分盘 1 时，目标设备实际读写“分盘 1.dd”的文件数据进行映射。计算机设备读取第 0 数据块时，则返回“分盘 1.dd”文件数据的首地址的 0 至后面的 512 个字节数据（单扇区大小为 512 字节），即返回文件数据块 0 的数据，以计算机设备操作的（扇区地址 $\times$ 512）为偏移量等方式，对文件数据进行读写。如果计算机能够直接读写文件对应的扇区数据，则直接读写对应的文件扇区。

需要说明的是，对于本实施例的文件分盘和下述实施例的联网分盘，扇区地址应扩大解释为“文件数据块”，即一个文件数据块对应一个扇区。例如：在单扇区大小为 512 个字节的情况下，读入扇区 0，则对应文件数据块 0，即读取文件的首地址至后面 511 字节的共 512 个字节数据；写入扇区 1，则对应文件数据块 1，等于从文件偏移量的 512 字节开始至后面的 511 个字节写入共 512 个字节数据。后续步骤不再赘述。

在一些实施例中，在图 1 所示实施例的基础上，图 16 示出了第七实施例提供的数据安全保护方法的流程示意图。与图 1 相同的步骤不再赘述，所述存储设备为联网存储设备，所述联网存储设备与服务端连接，所述服务端包含多个联网镜像文件，如图 16 所示，所述方法还包括：

步骤 S1001，将目标联网镜像文件作为存储数据源接入到所述计算机设备，所述目标联网镜像文件为多个所述联网镜像文件中的至少一个，所述存储数

据源包含所述目标文件。

在本实施例中，所述存储设备为联网存储设备，联网存储设备可以不存储数据，也可以存储数据，其通过有线方式或无线方式与服务端通信连接，所述服务端包含多个联网镜像文件。可选地，在基于分布式存储技术、优化
5 存储和 CDN 网络加速的情况下，联网镜像文件可以为数据库的数据，或者多个文件的组合、拼凑和映射等。

可选地，联网存储设备连接服务端，并向服务端发送标识信息，服务端根据联网存储设备的标识信息关联对应的联网镜像文件，在计算机设备发送数据交互指令时，向服务端转发数据交互指令的读写要求（例如读或写操作，
10 操作开始的扇区地址，连续读取扇区的长度），服务端接收到联网存储设备发送的读写要求后，返回联网镜像文件对应的扇区文件数据块地址，以实现联网存储设备的数据空间扩展。

可选地，根据联网存储设备的标识信息，在服务端切换控制联网存储设备对应的目标联网镜像文件，以将目标联网镜像文件接入到计算机设备。例如根据联网存储设备的标识号（或者用户的标识信息（通过账号登录绑定））
15 绑定“分盘 1.dd”、“分盘 2.dd”和“分盘 3.dd”3 个联网镜像文件，以在该 3 个联网镜像文件中切换接入到计算机设备的数据源。

示例性地，目标设备连接服务端，将服务端存储的“分盘 1.dd”的联网镜像文件接入到计算机设备，计算机设备以单扇区大小为 512 字节的方式发送数据交互指令，若该数据交互指令用于读取第 0 扇区地址的数据、向第 1 扇区地址写入数据，则保护模块向服务端发送请求，服务端将第 0 扇区转换为“分盘 1.dd”的首地址，将第 1 扇区转换为“分盘 1.dd”的第 512 个字节偏移量地址。
20 服务端根据转换后的地址，返回镜像文件“分盘 1.dd”首地址的 0 至后面的 511 个字节数据。向“分盘 1.dd”的第 512 个字节为偏移量地址至后面的 511 个字节数据写入数据，联网存储设备再将服务端返回的结果返回至计算机设备。
25

本实施例的联网存储设备能够在计算机设备无需安装软件工具的情况下随意切换不同的存储数据源，数据源的真实地址对计算机来说不可见，数据

源保存在云端，当联网存储设备丢失时可以远程取消数据源，提高数据存储设备的数据安全性。同时，本实施例直接读写服务端关联文件的特定偏移地址数据（或者文件对应的扇区地址数据，并以转发方式将数据直接转发至服务端或计算机设备，从而不受存储设备本身存储空间的限制，提高效率 and 5 增大适用场景。

在一些实施例中，采用描述符集合（及相关配置文件）区别以独立分盘形式、文件形式和联网形式等不同形式的数据源，从而让计算机设备能够区分不同的存储设备。“描述符集合”可以存储在数据源的隐藏位置，例如最后一个扇区并不能被计算机当作存储设备数据访问，也可以存储于服务端，还可以是存储于保护模块内置存储的某个扇区或者文件。 10

若保护模块设置在所述中间设备上；所述中间设备具有联网功能，以连接云端或服务端侧的存储模块。相应的，本申请实施例提供的方案中步骤“对所述数据交互指令做出响应”，包括：

将所述数据交互指令发送至网络侧存储模块，以便所述存储模块基于所述数据交互指令读取和/或写入相应的数据。 15

在一些实施例中，在图 13、15 和 16 任一实施例的基础上，所述方法还包括：

响应于用户输入的验证指令，将与所述验证指令的指令类型对应的目标存储数据源接入到所述计算机设备，所述目标存储数据源为扇区区间、镜像文件和联网镜像文件中的至少一种。 20

在本实施例中，验证指令为确定选中的目标存储数据源接入到计算机设备的指令，其可以携带有目标存储数据源对应密码信息。例如，目标存储数据源以分盘形式接入计算机设备为例，分盘 1 对应密码 A，分盘 2 对应密码 B，同时接入所有分盘的密码为 C，当验证指令携带密码 A 时，确认将分盘 1 接入到计算机设备；当验证指令携带密码 B 时，确认将分盘 2 接入到计算机设备；当验证指令携带密码 C 时，确认将分盘 1 和分盘 2 同时接入到计算机设备。本实施例通过在接入目标扇区区间时可以通过密码验证用户身份，以确 25

定接入选中的目标存储数据源，从而提高存储数据源的安全性。

在一些实施例中，在图 1 所示实施例的基础上，图 17 示出了第八实施例提供的数据安全保护方法的流程示意图。与图 1 相同的步骤不再赘述，如图 17 所示，所述方法还包括：

5 步骤 S1101，读取所述存储设备的用电需求信息；

步骤 S1102，根据所述用电需求信息，配置所述存储设备的电路限流保护策略，所述电路保护策略用于控制所述存储设备的用电状态。

在本实施例中，用电需求信息包括但不限于用电电流、用电电压和电路状态等，电路保护策略包括针对存储设备的保护策略和针对计算机设备的保护策略。

10 可选地，为了防止计算机设备输入大电流导致存储设备烧坏，所以根据存储设备的用电电流，配置保护策略，例如，中间设备连接计算机设备的第二接口与连接存储设备的第一接口之间的通路电流不超过用电电流，或不超过用电需求的预设允许上限（如 10%），又或者不超过预设固定值（如 500
15 毫安）。为了防止存储设备属于短路电路而导致计算机设备烧坏，所以根据存储设备的电路状态，配置保护策略，例如存储设备的电路状态为短路或者存在瞬时大电流时，中间设备断开与存储设备连接的第一接口的连接通路，或者增大与第一接口的电阻。

在一些实施例中，所述方法还包括：

20 生成交互日志，所述日志用于记录对于所述计算机发送的数据交互指令的处理记录。

在本实施例中，将计算机设备发送的数据交互指令的处理记录（例如记录转发情况、执行情况的相关数据）存储到交互日志中，以便于事后审计。

可选地，交互日志读出时可以配置为只读模式，使其无法被篡改，保证交互
25 日志存储记录的可靠性。

在一些实施例中，若当前保护模式为备份模式，相应的，步骤“对所述数据交互指令进行响应”可包括：

所述数据交互指令为写指令时，将所述计算机设备写入的数据同步写入至指定的备份存储区域内；和/或

所述数据交互指令为写指令时，保护模块在执行写入指令前，读取所述计算机设备写入的扇区地址数据并写入至指定的备份存储区域内。

- 5 上述“将计算机设备写入的数据同步写入至指定的备份存储区域”这样做的优点是：在计算机设备拷贝了重要数据，发现重要数据被另一个计算机设备恶意写入破坏的情况，此时就可以通过备份恢复进行数据恢复。

10 上述“保护模块在执行写入指令前，读取计算机设备写入的扇区地址数据并写入至指定的备份存储区域内”这样做的优点是：相当于在写入前保留原有的数据，在被计算机恶意删除或修改后，可以从备份存储区域内恢复。例如在引导扇区、FAT表、文件项信息等数据在计算机写入数据前预先进行备份，当发现被计算机恶意写入破坏后，在存储设备无法正常接入（如提示需要重新格式化）或文件将无法被正常显示或读写操作时，这时候可以通过备份恢复数据。

- 15 进一步的，当前保护模式为备份模式时，本申请实施例提供的数据保护方法还可包括如下步骤：

将接入存储设备的重要数据扇区的数据备份存储至指定的备份存储区域内；

- 20 当触发还原时，将所述指定的备份存储区域内的数据读出，写入至所述存储设备原有的数据扇区内。

其中，重要数据扇区可人为设定，比如用户可通过交互装置进行指定，被用户指定的数据扇区可标记为重要扇区。或者，重要数据扇区是保护模块自行设定；又或者，重要数据扇区是基于预置的重要性评判策略选定的，等等，本实施例对此不作具体限定。

- 25 参见图18a所示中间设备的一种结构形态实例。或者图18b所示的集成有具有本申请各实施例提供的保护方法对应功能的保护模块的存储设备。图18a和18b所示的中间设备在处于人工确认模式下可显示需人工确认的信息，

如文件名、文件类型、文件大小、操作等等。用户可通过“确认”控件进行确认操作，也可通过“取消”控件进行取消操作。按照不同的使用场景，使用人可在如图 18a 或 18b 所示的中间设备或存储设备的面板上手动操作：

- 一：选择保护模式。选择全盘只读，特定文件夹只写（空白文件夹）、
- 5 特定文件夹只读、特定文件夹读写等保护模式对应的保护开关，完成中间设备当前保护模式的设置。

二、选择物理数据源。选择数据源为 USB 存储设备、SD 卡、内置存储芯片或外部网络存储设备等等。

- 三、选择逻辑分盘数据源。进一步的将物理数据源的扇区地址进行切分，
- 10 形成多个数据源进行选择，选择其中一个分盘作为数据源。例如，一个 U 盘 16G，可以切割成 8G、4G、4G 的 3 个数据源。

四、中间设备接入计算机设备。将存储设备的 USB 公头接口插入到中间设备的 USB 母头接口，中间设备的 USB 公头插入到计算机设备的 USB 母头接口，使用计算机设备的 USB 接口为中间设备及存储设备供电。

- 15 图 19 示出了几种场景：

场景 1：计算机设备与存储设备之间通过中间设备连接，中间设备将计算机设备和存储设备隔离开。该场景 1 对应的中间设备的产品形态可以是一个类似于图 2a、2b 或 18a 所示的类似于一个接口转换器的硬件设备。

- 场景 2：中间设备的产品形态为读卡器，读卡器用于连接卡片类、芯片类
- 20 存储设备（如 SD 卡）。读卡器具有控制功能和保护功能，控制功能和保护功能可以是纯软件形式被集成在一颗芯片中，也可以是读卡器中的两个独立芯片。

- 场景 3、存储设备具有保护模块及内置至少一个或多个存储芯片（或存储颗粒），还有用于连接至少一个或多个外部存储设备的接口（如 TFCard 接口
- 25 用于接入 SD 卡、TF 卡，USB 接口用于接入 U 盘等）。其中，保护模块可以是独立芯片形式（如场景 4），也可以是类似于场景 5 中的纯软件形式被配置在存储设备的控制芯片上，还可以是场景 6 中的纯软件形式被配置在存储芯

片上等等，本实施例对此不作限定。若外部存储接口连接有存储设备，保护模块可根据需要切换物理数据源，如选择某个外部存储设备或某个存储芯片（或存储颗粒）。

场景 4、保护模块为移动存储设备硬件的一部分，但在硬件内部以保护芯片方式独立存在。例如，普通移动存储设备通过硬件升级，可以变为本发明申请的设备。

场景 5：数据安全保护方法的保护功能以软件方式集成在控制芯片中，即保护模块为软件形态。例如，普通移动存储设备通过控制芯片的软件（固件）升级，并安装外部按钮开关，可以变为本发明申请的设备。

10 场景 6：保护模块直接作为存储芯片的一部分，思路可以按照场景 4、场景 5 的软硬方式进行保护。目前有存储芯片带有保护功能的，例如可以设置只读的 SD 卡。

场景 7：数据安全保护方法的保护功能以软件方式集成在控制芯片中，即保护模块为软件形态。同场景 5 不同的是，数据存储设备没有控制芯片，所有的读写操作均由控制芯片直接完成。

这里需要补充说明的是：上文中提及了一种保护模式为逻辑分盘模式，在逻辑分盘模式下，保护模块会基于当前保护模式确定接入计算机设备的逻辑分盘（即逻辑意义上的数据源）。对于上述场景 3，保护模块设置在第一存储设备上，且第一存储设备上设有至少一个或多个存储芯片以及用于连接至少一个或多个外部第二存储设备的接口，所述第一存储设备上的至少部分接口连接有外部第二存储设备；相应的，保护模块当前保护模式指定的至少一个数据源可包括但不限于：

所述至少一个或多个存储芯片、所述第一存储设备上至少部分接口连接的外部第二存储设备中的至少一个物理数据源；和/或

25 所述至少一个或多个存储芯片中的至少一个逻辑分盘；和/或

所述第一存储设备上连接的外部第二存储设备中的至少一个逻辑分盘。

上文中提及本申请各实施例提供的技术方案中计算机设备与保护模块

间交互过程可包括但不限于：准备阶段、枚举阶段及数据交互阶段。参见图 20a 和 20b 所示，可简单总结出保护模块的基本运行逻辑如下：

第一阶段、物理存储数据源（存储设备）连接阶段。按照选择物理数据源，建立物理连接。如果保护模块为中间设备，则建立与存储设备的通信连接。如果存储设备为 SD 卡、TF 卡、内置存储芯片等，根据其接口（例如 SDIO、SPI、HSPI 等）建立通信连接。如果存储设备为 U 盘，保护模块根据其 USB 接口建立通信连接。如果存储设备为硬盘等，保护模块根据其 SATA、M.2 等接口进行连接。

第二阶段、保护模块读取物理存储数据源（存储设备）阶段，即上文中提及的准备阶段。在准备阶段，可预先分析存储设备。一种情况是：中间设备具有保护模块，计算机设备与存储设备通过中间设备连接；该情况下，保护模块读取存储设备数据并进行分析。另一种情况是：存储设备集成有保护模块，此时就不需要读取，直接对存储设备数据进行分析即可。如上文中对应的实施例，对存储设备的数据信息进行分析。更具体的，一是，读取描述符。如当保护模块为中间设备，物理数据源为 USB 接口的存储设备时，读取存储设备的设备描述符、配置描述符、接口描述符、端口描述符和字符串描述符，并判断是否为合法的设备类型，例如，大容量存储设备硬件类型。二是，读取存储设备的存储信息相关参数。如当物理数据源为 USB 设备、SD 卡、TF 卡、内置存储芯片等时，读取存储空间容量（或者为可用扇区大小）、读写权限等。三是、若保护模式为逻辑分盘模式时，按照存储空间建立扇区偏移关系。四是，当保护模式涉及文件系统时，进一步读取相关存储空间数据，如特定文件夹读写时，获取根目录首扇区地址和特定文件夹首扇区地址。例如，保护模式为特定文件模式时，根据文件系统的规则，寻找存储设备的特定文件夹的首扇区地址（或新建空白文件夹）、根目录（首目录）地址等用于映射的相关数据。

当第一阶段和第二阶段完成，且保护模块连接的设备的设备类型为允许接入的设备类型时，准备步骤成功，接口向计算机设备发送枚举信号，以进

入枚举阶段。参见图 20a 所示，基于存储设备的数据信息判定存储设备的设备类型，该步骤为计算机设备与存储设备之间通过具有保护模块的中间设备特有的。

即在本申请的一个具体的实施例中，所述目标设备为中间设备时，本申请提供的保护方法还可包括：在准备阶段，所述目标设备读取所述存储设备的数据信息并分析。若所述目标设备为存储设备时，所述方法还可包括：在准备阶段，所述保护模块对所述存储设备的数据信息进行分析。

参见图 20a 所示，在计算机设备向保护模块提供供电信号或保护模块启动时，便可进入准备阶段。若所述目标设备为中间设备，相应的上述步骤中“所述目标设备读取所述存储设备的数据信息”可包括：

在所述准备阶段，所述保护模块模拟所述计算机设备向所述存储设备发送控制指令；

接收所述存储设备反馈的所述存储设备的数据信息。

在一具体的可实施的技术方案中，“对数据信息进行分析”可包括：

基于所述数据信息，判定存储设备是否是所述当前保护模式指定的设备类型；

若是，则向计算机设备发送可以枚举信号，以进入枚举阶段。

第三阶段、枚举阶段。3.1、在枚举阶段，基于当前保护模式，对所述存储设备的数据信息进行处理，得到处理后信息；3.2、将处理后信息发送至所述计算机设备，以便建立所述计算机设备与存储设备间的通信连接。

其中，3.1“基于当前保护模式，对所述存储设备的数据信息进行处理，得到处理后信息”可具体包括：

3.1.1、根据当前保护模式，对所述数据信息进行处理，生成模拟所述存储设备的第二特征参数；和/或

3.1.2、根据当前保护模式，对所述数据信息进行处理，生成模拟所述存储设备的第二存储信息相关参数；

3.1.3、将所述第二特征参数和/或所述第二存储信息相关参数发送至所述

计算机设备，以便建立所述计算机设备与所述存储设备间的通信连接。

上述 3.1.1，在具体实施时可具体包括：获取所述当前保护模式对应的预设参数模板；根据所述数据信息中的第一特征参数反映出的所述存储设备的设备类型，从所述预设参数模板中获取能表征所述设备类型设备的至少一个参数项，以得到所述第二特征参数；或者利用所述当前保护模式对应的筛选策略，对所述第一特征参数中的参数项进行筛选，基于筛选出的至少一个参数项作，得到所述第二特征参数。

其中，所述第一特征参数可包括但不限于：描述符数据；其中，描述符数据包括如下中的至少一项：硬件描述符、接口描述符、端口描述符、端点描述符、字符串描述符等。

进一步的，所述数据信息包括第一存储信息相关参数，所述第一存储信息相关参数包括但不限于：存储设备可读写状态、可格式化块总数、最后逻辑块地址、单扇区字节数、最大逻辑单元数、设备信息。

上述 3.1.2，在具体实施时可具体包括：

3.1.2a、根据当前保护模式规定的操作类型，修改所述第一存储信息相关参数中的读写状态参数。

如图 21 所示的实例，②为保护模块向计算机设备返回的数据包，③是保护模块向计算机设备返回的状态包。其中，数据包中，保护模块对存储设备的读写状态参数进行了修改，如将读写状态 0x00 参数改为：0x80(代表只读)。

或者，保护模块直接向计算机设备返回只读（即写保护）状态。

这里需要补充说明的是：保护模块在数据交互过程中将读写状态参数进行了修改，这个修改位于保护模块的内存，并不修改存储设备的原始读写状态参数，也无需存储设备具有读写状态的修改权限（例如普通的 U 盘难以通过修改改变其读写状态）。

读写状态参数改为只读（写保护）状态后，计算机设备“认为”存储设备（例如 U 盘）为只读（写保护）状态，从而在人机交互界面中，禁止写操作。

3.1.2b、若所述当前保护模式为逻辑分盘模式，则根据当前保护模式规定

的可接入计算机设备的目标分盘的参数，修改所述第一存储信息相关参数中的可格式化块总数和/或最后逻辑块地址。

如图 22 所示的实例，②为保护模块向计算机设备返回的数据包，③是保护模块向计算机设备返回的状态包。其中，数据包中，保护模块对存储设备的可格式化块总数进行了修改，如把 0x01 DE 20 00 修改为 0x00 EF 10 00。图 22 所示的实例，是在逻辑分盘模式下，保护模块对存储设备的磁盘容量参数进行的修改。同样的，也可不修改，保护模块执行向计算机设备反馈含有 0x00 EF 10 00 的数据包。

其中，可格式化块总数可用于计算可格式化最大容量。例如，可格式化最大容量=可格式化块总数*每块字节长度。

这里需要补充的是：图 22 所示的实例可与附图 14d 对应着看。图 22 从数据处理过程视角，图 14d 是从物理视角来解释分盘 1 的情况。可见，在分盘 1 的情况下，将原有 16G 的存储空间的可格式化块总数进行修改，并返回给计算机，让计算机“认为”该存储设备仅有 8G。同样的，保护模块在数据交互过程中进行修改，修改数据仅位于保护模块的内存，并不修改存储设备的原始数据，也无需存储设备具有容量信息的修改权限（例如普通的 U 盘难以通过修改改变其容量信息）。

另外，图 23 示出了修改最后逻辑块地址的实例。如图 23 所示的实例，②为保护模块向计算机设备返回的数据包，③是保护模块向计算机设备返回的状态包。其中，数据包中，保护模块对存储设备的最后逻辑块地址进行了修改，如将 0x01 DE 1F FF 修改为 0x00 EF 0F FF。图 22 所示的实例，是在逻辑分盘模式下，保护模块对存储设备的磁盘容量参数进行的修改。同样的，也可不修改，保护模块执行向计算机设备反馈含有 0x00 EF 0F FF 的数据包。

3.1.2c、根据当前保护模式，修改所述第一存储信息相关参数中的设备信息，以保护存储设备的隐私信息。

图 24 示出了修改设备隐私信息的实例。如图 24 所示的实例，②为保护模块向计算机设备返回的数据包，③是保护模块向计算机设备返回的状态包。

其中，在设备隐私保护模式下，数据包中的有关厂商信息字符串、产品信息字符串、产品版本信息字符串等，均可改为 00.....00。同样的，也可不修改，保护模块执行向计算机设备反馈厂商信息字符串、产品信息字符串、产品版本信息字符串等为 00.....00 的数据包。

- 5 参见图 20a 和 20b 所示的枚举步骤中，计算机设备发送数据交互指令，以向保护模块请求获取硬件特征参数（即对应上文中提及的存储设备的第一特征参数）。具体的，该硬件特征参数可以包括但不限于：硬件描述符、接口描述符、端口描述符、端点描述符、字符串描述符等。保护模块基于在准备阶段获取到的数据信息，结合当前保护模式对数据信息中的第一特征参数
- 10 进行数据处理，得到第二特征参数并向计算机设备返回所述第二特征参数。进一步的，计算机设备继续发送数据交互指令，以向保护模块请求获取存储设备的存储信息相关参数。其中，存储信息相关参数可包括但不限于：设备可读写状态、可格式化最大容量和/或可格式化块总数（图中未示出）、最后扇区地址、单扇区字节数、最大逻辑单元数、设备信息（图中未示出）等等。
- 15 保护模块基于在准备阶段获取的数据信息，结合当前保护模式对数据信息中的第一存储信息相关参数进行数据处理，得到第二存储信息相关参数并向计算机设备返回所述第二存储信息相关参数。

- 参见图 20b 所示，枚举阶段又可细分为：建立接口连接子阶段和读取存储设备信息子阶段。在建立接口连接子阶段：1 访问控制，根据预设访问控制
- 20 规则，读取存储设备的描述符数据（即上文中提及的第一特征参数），判断是否符合预设要求。若符合预设要求，允许计算机设备与存储设备建立连接；否则，禁止计算机设备与存储设备建立连接。2、内容修改，根据内容修改规则（如上文中提及的 3.1.1），向计算机设备返回已修改或替换后的描述符数据。在读取存储设备信息子阶段：1、访问控制，根据预设访问控制规则，读
- 25 取存储设备的存储信息数据（即上文中提及的存储信息相关参数），判断是否符合预设要求。若符合预设要求，允许计算机设备与存储设备建立连接；否则，禁止计算机设备与存储设备建立连接。2、内容修改，根据内容修改规

则（如上文中提及的 3.1.2a~3.1.2c），向计算机设备返回已修改或替换后的存储信息数据。

第四阶段：数据交互阶段。参见图 20a 所示，计算机设备向保护模块发送数据交互指令（如读指令），该数据交互指令可包括：读指令及扇区地址。

- 5 如果该扇区地址禁止读，则保护模块不发送数据交互指令至存储设备。如果该扇区地址在符合规则的情况下（即可读），将扇区地址修改为规则预设的扇区地址（如逻辑分盘、特定文件夹读等）。存储设备返回修改后的扇区地址对应的数据（读出数据+读状态）。保护模块将存储设备返回的数据发送至计算机设备。继续参见图 20a，计算机设备向保护模块发送数据交互指令（如写指令），该数据交互指令可包括：写指令、扇区地址及写入数据。如果该扇区地址禁止写，则保护模块不发送数据交互指令至存储设备。如果该扇区地址在符合规则的情况下（即可写），将扇区地址修改为规则预设的扇区地址（如逻辑分盘、特定文件夹读写等）。若当前保护模块为加密写入模式，还需要对要写入的数据进行加密处理后再写入修改后的扇区地址对应的位置。
- 10 存储设备返回写状态。保护模块将存储设备返回的写状态发送至计算机设备。

- 图 20b 是从三方面对数据交互阶段进行的说明。参见图 2b 所示的实施例，在数据交互阶段：判断计算机的读/写扇区地址是否符合预设要求（如上文中提及的是否禁止写、禁止读等），来进行访问控制。若符合访问控制规则，则允许计算机设备对扇区地址进行读/写操作；否则，禁止计算机设备对扇区地址进行读/写操作。随后，进行地址映射，根据地址映射规则，即上文中提及的扇区地址修改规则，读写存储设备相应的被映射扇区地址的数据，并向计算机设备直接返回读数据或写状态。或者，还可进行内容修改，即根据内容修改规则，读/写存储设备相应扇区地址的数据进行修改，并向计算机设备返回读数据或写状态。
- 20

- 25 下面举一个具体实例，在计算机设备被允许与存储设备建立连接后，计算机枚举读取存储设备的流程可包括但不限于如下内容：

1、计算机设备读取存储设备的 0 扇区，分析 MBR 或 GPT 扇区或文件系

统引导扇区的数据，获取文件系统分区信息的扇区地址；

2、读取文件系统分区信息的扇区地址，根据文件系统的协议，分析出根目录（或称为首目录）首扇区地址；

3、根据文件系统协议，读取根目录扇区地址数据；

5 4、分析根目录扇区地址数据的文件和文件夹信息；

5、在计算机设备中显示根目录的文件和文件夹列表。

参见 28a~28d 分别示出了访问控制过程的示例。图 28a 示出了数据处理过程视角下控制“读指令（单扇区读）”扇区地址、数据包或者状态的示意图。图 28b 示出了数据处理过程视角下控制“读指令（多扇区连续读）”扇区地址、数据包或者状态的示意图。图 28c 示出了数据处理视角下控制“写指令（单扇区写）”扇区地址、数据包或状态。图 28d 示出了数据处理视角下控制“写指令（多扇区连续写）”扇区地址、数据包或状态。

具体的，参见图 28a 所示，计算机设备发送的指令（或指令包、CBW 包），以 SCSI 协议为例，0x28 代表：READ(10)指令，请求读取扇区地址数据。该指令中还包含有操作扇区地址 00 00 00 00 及操作扇区数量 00 01。保护模块结合操作扇区地址 00 00 00 00 及操作扇区数量 00 01，若判断该扇区地址对应的读权限在当前保护模式下为禁止读，则不进行实际读操作，例如扇区限位模式、逻辑分盘模式等。若保护模块当前保护模式为逻辑分盘模式、特定文件模式、空白文件模式等，则调整实际操作扇区地址（如上文提及的映射方式）。若保护模块当前保护模式还组合有其他模式或判断，则触发其他模式，如解密读出模式、异常判断等。如图 28a 所示保护模块在响应计算机设备发送的指令时，判断该指令欲读取扇区的数据是否符合当前保护模式要求，例如文件类型限制模式中限定的文件类型等。保护模块可基于当前保护模式，整块修改或逐字修改，该修改可以不修改该扇区原有的数据，例如解密读取模式、文件类型限制模式等。进一步的，保护模块还可基于其他模式对欲返回给计算机设备的数据（或数据包、DATA 包）进行辅助修改，例如特定文件模式下修改根目录地址等。保护模块除向计算机设备返回数据外，还返回状

态包（或 CSW 包）。具体的，若操作扇区地址不具备操作权限，则可以不返回真实数据包，可以将该字节为非 0x00，并直接返回状态包；或者返回非真实的数据包，并直接返回该字节 0x00 的状态包，使计算机设备认为读取成功。

参见图 28b 所示，计算机设备发送的指令（或指令包、CBW 包），以 SCSI

- 5 协议为例，0x28 代表：READ(10)指令，请求读取扇区地址数据。该指令中还包含有操作扇区地址 00 00 00 00 及操作扇区数量 00 02。即图 28b 为多扇区连续读指令对应的控制。保护模块的控制过程同上述图 28a，区别仅在于：图 28b 在多扇区连续读取过程中，可进行逐扇区操作。

- 参见图 28c 所示，计算机设备发送的指令（或指令包、CBW 包），以 SCSI
- 10 协议为例，0x2A 代表：WRITE(10)指令，请求将数据写入扇区地址。在全盘只读模式下，不执行该指令（即该指令被禁止）。该指令中包含有操作扇区地址 00 00 08 D8 及操作扇区数量 00 01。保护模块结合操作扇区地址 00 00 08 D8 及操作扇区数量 00 01，若判断该扇区地址对应的写权限在当前保护模式下为禁止写，则不进行实际写操作，例如扇区限位模式、逻辑分盘模式等。
- 15 若保护模块当前保护模式为逻辑分盘模式、特定文件模式、空白文件模式等，则调整实际操作扇区地址（如上文提及的映射方式）。若保护模块当前保护模式还组合有其他模式或判断，则触发其他模式，如解密读出模式、异常判断等。如图 28c 所示保护模块在响应计算机设备发送的数据包（或 DATA 包）时，判断该欲写入数据的扇区的数据是否符合当前保护模式要求，例如
- 20 文件类型限制模式中限定的文件类型等。保护模块可基于当前保护模式，整块修改或逐字修改，例如加密写入模式、文件类型限制模式等。保护模块还向计算机设备返回状态包（或 CSW 包）。具体的，若操作扇区地址不具备写操作权限，则可以不返回真实数据包，可以将该字节为非 0x00，并直接返回状态包；或者直接返回该字节 0x00 的状态包，使计算机认为写入成功。参见
- 25 图 28d 所示，计算机设备发送的指令（或指令包、CBW 包），以 SCSI 协议为例，0x2A 代表：WRITE(10)指令，请求将数据写入扇区地址。该指令中还包含有操作扇区地址 00 00 08 D8 及操作扇区数量 00 02。即图 28d 为多扇区

连续写指令对应的控制。保护模块的控制过程同上述图 28c，区别仅在于：图 28d 在多扇区连续写入过程中，可进行逐扇区操作。

总结一下，本申请各实施例提供的技术方案的优势在于：

优势一、应用场景方面

- 5 通用性强，能够对市面上通用的移动存储设备进行保护，例如 U 盘、USB 光驱光盘、SD 转接器、SD 卡等，保护的设备兼容性高。

可行性高，在计算机设备无需安装特定软件就能保护，对于存储设备使用来说，保护的可行性高。

- 10 应用广，可以广泛应用在内网环境、工业控制设备、打印机设备、物联网设备等众多场景的设备中，并无需对已有的系统或软件进行升级，能够使用现有嵌入式设备或操作系统自带的驱动程序，保护的计算机设备场景多。

优势二、安全性方面

保护模块按照设置采用接入设备的硬件参数特征，计算机设备的恶意程序无法发现保护模块的存在，无法对保护模块的接入进行限制。

- 15 保护模块的软件为无操作系统、固件的方式，对保护模块进行提权，无法对软件进行篡改和删除。

保护的方式位于设备间通信的底层，恶意程序无法绕过保护措施。

保护的过程可以被日志审计，可以将计算机设备与存储设备的所有的操作命令和数据包在保护模块内置存储进行保存，可以进行事后审计。

- 20 保护持久稳定性强，保护是基于底层的通信协议进行控制，在保护模块出厂后即可完成保护功能，不需要进行病毒库的升级和后期维护工作。

优势三、保护模式方面

保护的覆盖面广，从物理层、通信层、文件系统层均能够进行保护；

保护的方式多，可以分为只读、只写或自定义模式；

- 25 保护的颗粒度细，能具体到特定文件、文件夹或扇区地址区间进行保护。

具体保护模式的实现方式：

具体实施方式：基本保护，接入设备类型判断。

在存储设备接入保护模块，保护模块接入计算机设备通电后，保护模块通过 USB0 接口，模拟计算机设备的控制传输指令，读取存储设备的设备描述符、配置描述符、接口描述符、端点描述符。如果获取上述描述符成功，就按照正常大容量存储设备（U 盘、移动光驱等存储设备的标准设备类型）

5 的特征进行判断，例如判断（判断可以是单一条件或组合条件）：

1.1、判断设备的接口类型是否为“Mass Storage Class”（USB 标准协议，大容量存储设备类型），具体为判断接口描述符的第 6 个字节，确认是否为 0x08（大容量存储设备）

1.2、判断设备的接口子类是否为“SCSI transparent command set”（SCSI
10 传输协议，根据存储设备不同有所不同），具体为判断接口描述符的第 7 个字节，确认是否为 0x06（SCSI 通信子类）

1.3、判断设备的接口协议是否为“Bulk Only Transport”（USB 标准协议，批量传输协议），具体为判断接口描述符的第 8 个字节，确认是否为 0x05（批量传输）

15 1.4、判断设备的所有端点是否为“Bulk”（USB 标准协议中的批量传输协议），具体为判断接口描述符的第 4 个字节，确认是否为 0x02（批量传输）。

如果不符合大容量存储设备的设备描述符特征的，接入的“存储设备”可能实际上为单一功能的鼠键等输入设备，或者是带有鼠键功能和大容量存储功能的设备，这种情况下，中间设备终止与存储设备进行进一步的通信。

20 同时，在后续环节通过生成虚拟“虚拟移动盘”设备的方式，在操作系统显示“非正常设备”的字符串盘符名，并在虚拟移动盘的根文件保存读取的该“存储设备”的原始硬件参数数据的文本文件以供分析。

在符合正常大容量存储设备的设备描述符的情况下，通过模拟移动存储设备的硬件参数和特征，使计算机设备读取保护模块的数据与原始的移动存储设备完全一致，计算机设备不会识别出中间设备的存在，避免恶意程序对
25 中间设备进行拦截。

举例来说，如图 25 所示，中间设备的 USB0 有设备接入时，判断是否符

合正常的大容量存储设备特征，若符合，则对应上述图 19 中的场景 3~6 直接获取硬件特征参数，而对应上述图 19 中的场景 1~2 获取大容量存储设备的硬件特征参数。随后，将内置的设备描述符、配置描述符模板，将 USB0 设备（即存储介质）的厂商 ID、设备 ID、字符串等进行替换填充；最后按照硬件特征参数向 USB1 端连接计算机设备模拟 USB0 接入设备（即存储介质）。若不符合，则终止与存储设备或存储介质的通信；并通过“虚拟盘”的盘名称向 USB1 端口的计算机设备显示盘符，提示为非正常设备。在虚拟盘的根目录保存读取的该“移动存储设备”的原始硬件参数数据的文本文档；硬件初始化失败。

10 图 26a 示出了本申请各实施例提供的技术方案相关技术点的整理图。图 26b 示出了采用本申请各实施例提供的技术方案带来的一些效果。

图 27 示出了另一个具体实例，场景 1 对应存储介质分盘场景。计算机设备向中间设备发送数据交互指令，例如发送读取地址 0 数据，读取数据长度 512 字节；写入地址 1 数据，写入数据为 0x1212...（512 字节），写入数据长度 512 字节。中间设备接收到后，将数据交互指令操作扇区地址进行转化，例如将地址 0 转化 1000，地址 1 转换为 1001，对转化后地址对应的扇区进行操作，如返回地址 1000 的数据，向地址 1001 写入数据...（512 字节）。若场景 1 中与计算机设备连接的是具有保护模块的存储设备，则中间框对应的可以是存储设备中的保护模块，图 27 中最右侧的框为存储设备（如 U 盘、TF 卡、SD 卡等）或存储介质（如存储芯片、存储颗粒等）。

场景 2 对应存储介质文件分盘场景。计算机设备向中间设备发送数据交互指令，例如发送读取地址 0 数据，读取数据长度 512 字节；写入地址 1 数据，写入数据为...（512 字节），写入数据长度 512 字节。中间设备接收到后，结合地址、单个扇区字节数（例如为 512 字节）、数据长度计算，将数据交互指令操作扇区地址转换成文件数据对应的地址，例如转化为对 U.dd 文件数据的读写操作。例如，地址 0 转化为 U.dd 文件数据的 0 扇区地址，地址 1 转换为 U.dd 文件数据的 1 扇区地址，转化后对 U.dd 文件数据进行操作，如返

回 U.dd 文件地址 0 扇区的数据, 向 U.dd 文件数据扇区地址 1 写入数据 0x1212...

(512 字节)。同样的, 若场景 2 中与计算机设备连接的是具有保护模块的存储设备, 则中间框对应的可以是存储设备中的保护模块, 图 27 中最右侧的框为存储设备 (如 U 盘、TF 卡、SD 卡等) 或存储介质 (如存储芯片、存储颗粒等)。

场景 3 对应存储介质文件分盘 (联网) 场景。计算机设备向中间设备发送读写交互指令, 例如发送读取地址 0 数据, 读取数据长度 512 字节; 写入地址 1 数据, 写入数据为 0x1212... (512 字节), 写入数据长度 512 字节。中间设备接收到后, 结合地址、单个扇区字节数 (例如为 512 字节)、数据长度计算, 将数据交互指令操作扇区地址转换成服务端数据对应的地址 (或者由服务端根据转发的数据交互指令, 按照预设的规则进行转换), 例如转化为对服务端的 U.dd 文件数据的读写操作。例如, 地址 0 转化为服务端的 U.dd 文件数据的扇区 0 地址, 地址 1 转换为服务端的 U.dd 文件数据的扇区 1 地址, 转化后对服务端的 U.dd 文件数据进行操作, 如返回服务端的 U.dd 文件数据地址 0 的数据, 向服务端的 U.dd 文件数据扇区地址 1 写入数据 0x1212... (512 字节)。同样的, 若场景 3 中与计算机设备连接的是具有保护模块的存储设备, 则中间框对应的可以是具有联网能力的存储设备。

再有, 本申请实施例还提供一种安全控制框架。按照图 20a、20b、21-24 以及图 28a~图 28d 读写控制, 根据业务场景对准备阶段、枚举阶段、数据交换阶段的数据交互指令、数据和状态进行允许禁止控制、编辑修改等, 以达到控制的目的。

安全控制框架是位于计算机设备与存储设备中间的保护模块, 可以根据保护场景 (或业务场景) 需要, 配置不同的保护方式, 并根据实际情况进行切换。在准备阶段、枚举阶段、数据交互阶段中, 实现对计算机设备、存储设备或计算机设备和存储设备的信息安全保护。同时, 安全控制框架的保护场景可以基于本发明的保护模式进行单独使用或者组合使用, 也可以按照实际需要创建出新的保护场景 (保护模式); 多个保护场景同时组合保护, 或

者由保护场景触发启动另一保护场景。

需要说明的是，本申请的保护方法、保护模式以及相关实施例，可以基于安全控制框架进行配置创建，也可以根据保护方法独立存在。

在一个具体的实施例中，所述安全控制框架包括：

5 配置模块，用于配置保护场景；

生成模块，用于生成保护场景的配置信息或带有所述保护场景的软件；

其中，一种保护场景对应至少一种保护模式；将所述配置信息或带有所述保护场景的软件部署在硬件设备上，使得所述硬件设备具有本说明书中所述数据安全保护方法中的步骤对应的功能。

10 进一步的，配置模块在配置保护场景时，具体用于：

配置保护场景标识信息；

配置所述保护场景对应的保护操作的策略。

上述“配置所述保护场景对应的保护操作的策略”，可包括但不限于至少一个或多个：

15 配置所述保护场景下准备阶段内保护操作的策略；

配置所述保护场景下枚举阶段内保护操作的策略；

配置所述保护场景下数据交互阶段内保护操作的策略。

再进一步的，本实施例提供的所述安全控制框架还可包括：编译模块，用于根据所述配置信息执行相应的软件编译策略得到安全控制软件；其中，

20 硬件设备运行该安全控制软件，使得硬件设备具有上述权利要求 1~44 中任一
项所述数据安全保护方法中的步骤对应的功能。当然，安全控制框架也可没有编译模块。保护场景的配置信息可导入至硬件设备（如新型 U 盘或如图 2a 所示的中间设备等），硬件设备具有编译能力，根据配置信息执行相应的软件编译策略以生成安全控制软件（或可成为安全控制程序），以便于执行实
25 现如上文各实施例中提及的保护模块对应的功能。

具体的：

一、配置保护场景

保护场景的配置包括：

（一）保护场景信息，如名称、编号、二进制值等，用于作为选定保护场景的唯一标识；如备注信息、字符串信息等，用于场景数据的管理等。

（二）配置保护操作的策略，包括以下至少一个或者多个的组合：

- 5 1.在准备阶段的策略。保护模块对存储设备的读取，经过提取、分析、修改等方式，获取保护场景所需的数据。

配置用于准备阶段向连接的存储设备的数据交互指令（相当于保护模块向存储设备发送哪些数据交互指令），用于向存储设备请求数据或写入数据。

- 10 配置匹配符合存储设备返回的数据的判断、修改或响应方案（相当于当匹配到的存储设备返回的数据要进一步怎么做）。

在准备阶段的策略可包括但不限于：数据交互指令发送策略、数据交互指令执行结果策略等。

- 15 （1）配置数据交互指令发送策略。设置用于模拟计算机控制存储设备的至少一个或多个数据交互指令。数据交互指令包括但不限于：USB 标准请求（例如获取设备描述符、配置描述符、接口描述符、端口描述符、字符串描述符请求等），类特殊请求（例如 Bulk-Only Mass Storage Reset、Get Max LUN 请求等），SCSI 命令集和 UFI 命令集请求（例如 INQUIRY 请求、READ FORMAT CAPACITIES 请求、READ CAPACITY 请求、READ (10) 命令、WRITE (10) 命令等），以及自定义请求或命令等等。

- 20 （2）配置匹配数据交互指令执行结果策略。设置用于识别数据交互指令执行结果返回数据的至少一个或多个数据特定位置的字节值，并绑定匹配后的处理策略。数据交互指令执行结果数据包括但不限于：USB 标准请求返回数据（例如设备描述符、配置描述符、接口描述符、端口描述符、字符串描述符等），类特殊请求返回结果（例如最大 LUN 数量等），SCSI 命令集和 UFI
25 命令集请求（例如可格式化块总数、最后逻辑块地址、单扇区字节数、扇区位置读出的数据和状态、扇区位置写入数据的状态等），以及自定义请求或命令等等。

处理策略包括：

①数据是\否判断。预设数据交互指令规则并发送，对预设返回数据的至少一个或多个特定位置（例如特定位置的字节值）的数据进行判断，如果符合预设则进行操作 A，如果不符合则进行操作 B。例如，在硬件类型接入保护模式（保护场景）中，可以通过读取描述符等数据进行判定是否符合接入要求，当不符合时断开与存储设备通信；当符合时向计算机设备发送可以枚举的信号。

②数据修改\保存。预设数据交互指令规则，实现对预设返回数据的至少一个或多个特定位置（例如特定位置的字节值）的数据进行修改保存。例如，存储设备的数据信息保护模式或设备隐私保护模式（保护场景）中，可以通过读取描述符等数据进行修改并在保护模块中保存。

③数据提取\分析。预设数据交互指令规则并发送，实现对至少一条或多条数据交互指令返回数据的上下文分析，提取或计算最终数值。例如，在特定文件模式、文件类型限制模式、人工确认模式等模式（保护场景）中，可以通过读取文件系统的数据，分析根目录或者相关文件的扇区地址区间。

④数据写入。预设数据交互指令规则并发送，实现结合数据提取\分析的结果，对特定扇区地址写入预设的数据。例如空白文件模式中，在特定扇区地址空间写入文件项相关的数据，以实现自动创建文件夹的目的。

2.在接入阶段的策略。计算机设备与保护模块建立通信连接（计算机主机枚举），为数据交换做准备。

配置用于匹配接入阶段的数据交互指令（相当于哪些交互指令需要进行响应），配置符合匹配结果时的判断、修改或响应方案（相当于当匹配到的数据交互指令要进一步怎么做）。

（1）配置计算机设备发送的数据交互指令匹配策略：设置用于识别数据交互指令的至少一个或多个数据特定位置的字节值，并绑定匹配后的处理策略。数据交互指令包括指令数据和数据包数据，例如指令请求包和回复数据包。当读取数据交互指令数据时，判断至少一个或多个数据位置的字节值，

当数据交互指令符合匹配项时，执行绑定的处理策略。

判断的数据交互指令为：配置计算机设备发送的用于建立连接的请求。
例如 USB 标准请求，以及用于获取设备描述符、配置描述符、接口描述符、端口描述符、字符串描述符、或其他自定义描述符的数据交互指令。具体的，

5 例如 USB 标准请求数据共有 8 个字节，分为 5 个部分。

标准请求数据	第 0 字节	第 1 字节	第 2-3 字节	第 4-5 字节	第 6-7 字节
数据项名称	RequestType	Request	Value	Index	Length
示例数据	0x80	0x60	0x00 0x01	0x00 0x00	0x12 0x00

按照 USB 标准请求规定，当 Request（第 1 字节位置）为 0x06 时，则为获取设备描述符。为此可以判断第 1 字节位置是否为 0x06，当匹配时，执行绑定请求设备描述符的处理策略。USB 标准请求（例如获取设备描述符、配置描述符、接口描述符、端口描述符、字符串描述符等）或非标准请求（获取自定义的描述符等）以此类推。

10 (2) 配置匹配数据交互指令执行策略，主要包括：

①指令是\否执行判断。预设数据交互指令规则，实现选择进行操作 A，或选择进行操作 B。例如，在数据交互指令为请求设备描述符时，回复设备描述符数据；数据交互指令不符合时，不回复数据。

15 ②数据不修改\修改\替换回复。预设数据交互指令规则，实现回复存储设备原数据、或者回复经预设规则修改的数据、或者回复预设固定的替换数据。
例如，在存储设备的数据信息保护模式（保护场景）、数据信息保护模式或设备隐私保护模式（保护场景）等模式中，回复修改或替换后的描述符等数据；在只读模式（保护场景）等模式中，修改读写状态信息（如图 21 所示）；
20 在逻辑分盘模式（保护场景）等模式中，修改容量相关信息（如图 22、图 23 所示）。

④执行对存储设备、存储介质的数据读取/写入操作。预设数据交互指令规则，实现执行对存储设备预设的读/写操作。例如，当接收到预设的数据交互指令（可能具有危险性的数据交互指令）时，优先执行对存储设备扇区数

据的读/写操作，提前做好数据保护。

⑤执行触发启动保护模式。预设数据交互指令规则，实现执行启动保护模式的操作。例如，当接收到预设的数据交互指令（可能具有危险性的数据交互指令）时，启动备份模式，防止数据遭到破坏；启动日志记录，保存数据交互指令日志信息。

⑥执行断开计算机设备操作。预设数据交互指令规则，实现执行断开计算机设备连接操作。例如，当接收到预设的数据交互指令（可能具有危险性的数据交互指令）时，断开计算机设备连接。

⑦执行虚拟存储介质操作。预设数据交互指令规则，实现在数据交换阶段连接至虚拟存储介质。例如，当接收到预设的数据交互指令（可能具有危险性的数据交互指令、或者为禁止连接的设备类型）时，在后续数据交换阶段，将数据操作连接至虚拟存储介质（非真实数据的存储介质）进行响应，其中虚拟存储介质可以为带有相关提醒信息的“虚拟盘”，也可以为有普通存储介质形态的“虚拟盘”。

⑧执行触发选定数据源。预设数据交互指令规则，实现选定存储设备、存储介质或者逻辑分盘。例如，当接收到预设的数据交互指令时，选定预设的存储设备、存储介质或者逻辑分盘，作为接入数据源。

3.在数据交互阶段的策略。计算机设备与保护模块进行数据交换，主要为计算机设备向保护设备发送读/写扇区地址相关的数据交互指令。

配置用于匹配数据交换阶段的数据交互指令（相当于对读/写数据交互指令或者其他用于数据交换阶段的数据交互指令的响应），配置符合匹配结果时的判断、修改或响应方案（相当于匹配到的数据交换指令（读/写等）要进一步怎么做）。

（1）配置计算机设备发送的数据交互指令匹配策略：设置用于识别数据交互指令的至少一个或多个数据特定位置（或参数）的字节值，并绑定匹配后的处理策略。

数据交互指令包括指令数据、数据包数据和状态包数据，例如读取指令

和回复的数据包、回复的状态包；写入指令、写入的数据包和回复的数据包。

判断的数据交互指令主要对应的至少一个或多个数据特定位置（或参数）的字节值。如图 28a~28d 中的①②③或①②③④的所有数据。对于指令①（计算机设备发送指令（指令包）（CBW 包））来说，根据不同的场景主要判断传输的总字节数、传输方向、操作的 LUN、命令块长度、操作指令代码、操作 LUN、操作扇区地址、操作扇区数量。对于一个或多个数据包来说，根据不同的场景判断特定位置的字节值，或者特定数据区间的多个字节值或哈希值。对于状态包来说，主要判断剩余字节数、执行的错误代码。

参见图 28a~28d，图 28a 示出了数据处理过程视角下控制“读指令（单扇区读）”扇区地址、数据包或者状态的示意图。图 28b 示出了数据处理过程视角下控制“读指令（多扇区连续读）”扇区地址、数据包或者状态的示意图。图 28c 示出了数据处理视角下控制“写指令（单扇区写）”扇区地址、数据包或状态。图 28d 示出了数据处理视角下控制“写指令（多扇区连续写）”扇区地址、数据包或状态。

上述图 28a~28d 示出的数据处理过程涉及的 CBW、DATA、CSW、操作指令代码均属于 SCSI 协议。图 29 示出了计算机设备、保护模块及存储设备（如 U 盘、存储卡或存储芯片）的连接示意图。对于保护模块与存储设备的连接，其实只是接口和协议不同，本质上都是“中间设备或读卡器”原理。包括我们现有的 U 盘、移动硬盘等，实际上也是内置存储芯片的读卡器而已，技术逻辑是控制芯片将接收到的 SCSI 指令转换成能够读/写存储介质的 SDIO 或 SPI 的指令，并操作存储介质的数据。但是，如果是控制+存储是分离式的，例如 U 盘、读卡器，中间设备需要在准备阶段预先获取存储信息。对于 USB 接口的 U 盘也需要对描述符进一步判断，确定 U 盘的设备类型（单纯的大容量存储设备类型），确保没有 HID 等功能；如果是控制+存储是集成式的，例如本发明的新型 U 盘，存储信息预先是固定的，准备阶段就无需再获取，但如果为逻辑分盘模式，也需要修改容量信息，如果为特定文件夹读写模式，也需要进行文件地址的读取。

(2) 配置匹配数据交互指令执行策略，主要包括：

- ①指令数据是\否执行判断。预设数据交互指令规则，实现选择进行操作 A，或选择进行操作 B 等判断。例如，在只读模式（保护场景）等模式中，当
5 计算机设备发送数据交互指令写入数据时（如操作指令代码为 0x2A（写数据）），
保护模块不执行写操作。例如，在扇区限位模式（保护场景）等模式中，当
计算机设备发送数据交互指令操作扇区地址（结合操作扇区数量计算，可以
同时对多组数据进行综合判断）处于预设的只读\只写限制时，保护模块不执
行相应的操作。
- ②指令数据修改\替换。预设数据交互指令规则，实现修改或替换指令数
10 据，再将指令数据发送至存储设备。例如，在逻辑分盘模式、特定文件模式、
空白文件模式中，根据预设修改操作扇区地址并读写对应的存储设备扇区地
址。
- ③数据包是\否转发判断。预设数据包规则，实现选择进行操作 A，或选
择进行操作 B 等判断。例如，在文件限制读写中，可以预设关键字比对规则，
15 数据包内容命中比对规则的转发\或不转发至计算机设备\或存储设备。
- ④数据包数据修改\替换。预设数据包规则，实现修改或替换数据包数据，
再将数据包发送至计算机设备\或存储设备。例如，在加密写入或解密读出模
式中，按照预设规则对数据包数据进行修改，再转发至计算机设备\或存储设
备。例如，在扇区限位读写模式中，可以按照预设规则，当计算机设备读取
20 的扇区地址不符合预设规则时，直接返回预设用于替换的数据包（例如空白
数据包）。
- ⑤状态包是\否转发判断。预设数据包规则，实现选择进行操作 A，或选
择进行操作 B 等判断。例如，判断状态错误代码未非 0x00 时，是否将状态包
转发至计算机设备。
- ⑥状态包数据修改\替换。预设数据包规则，实现修改或替换状态包数据，
25 再将状态包发送至计算机设备\或存储设备。例如，在扇区限位读写模式中，
可以按照预设规则，当计算机设备读取的扇区地址不符合预设规则时，直接

返回预设用于替换的状态包（例如非 0x00 错误状态的数据包）。

- ⑦执行对存储设备、存储介质的数据读取/写入操作。预设数据交互指令判断规则，实现执行对存储设备预设的读/写操作。例如，当接收到预设的数据交互指令（例如可能是具有危险性的指令、数据包或状态包）时，优先执行对存储设备扇区数据的读/写操作，提前做好数据保护。

⑧执行触发启动保护模式。预设数据交互指令判断规则，实现执行启动保护模式的操作。例如，当接收到预设的数据交互指令（例如可能是具有危险性的指令、数据包或状态包）时，启动备份模式，防止数据遭到破坏；启动日志记录，保存数据交互指令日志信息。

- ⑨执行断开计算机设备操作。预设数据交互指令判断规则，实现执行断开计算机设备连接操作。例如，当接收到预设的数据交互指令（例如可能是具有危险性的指令、数据包或状态包）时，断开与计算机设备连接。

- ⑩执行触发选定数据源。预设数据交互指令判断规则，实现重新选定存储设备、存储介质或者逻辑分盘。例如，当接收到预设的数据交互指令（例如可能是具有危险性的指令、数据包或状态包）时，重新选定预设的存储设备、存储介质或者逻辑分盘，或者虚拟存储介质（非真实数据的存储介质），并断开设备重新进行枚举作为接入数据源。

二、生成保护场景的配置信息或者带有保护场景的软件

针对上述配置的保护场景信息和保护操作策略：

- 一方面可以生成配置信息。生成导出配置信息，通过数据传输（例如网络传输、点对点传输、复制拷贝）等方式进行共享。根据不同使用场景可以进一步进行修改配置信息。配置信息能够导入安全控制框架软件或安全控制框架硬件设备中，由安全控制框架执行相应安全控制策略。

- 另一方面可以生成软件（或固件）。在安全控制框架的软件或硬件设备中，根据自行编写或从外部导入的配置信息执行相应的软件编译策略，将配置信息中的保护场景生成安全控制软件（或固件）。通过将安全控制软件（或固件）在操作系统或硬件设备上运行，执行相应安全控制策略。

三、执行保护场景安全控制

安全控制软件（或固件）或安全控制框架软件（或固件）成为保护模块，在操作系统、硬件设备、控制芯片、存储芯片等设备上运行。

在准备阶段，根据保护场景配置，向存储设备发送数据交互指令。

- 5 在枚举阶段、数据交互阶段中，根据保护模块当前的保护场景（保护模式），对计算机设备发送的数据交互指令进行权限控制，所述数据交互指令用于所述计算机设备与所述存储设备进行数据交互；

若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应。

10

另外，本申请还一实施例提供一种中间设备。该中间设备包括：

第一端口，用于连接计算机设备；

第二端口，用于连接存储设备；

交互模块，包括如下中的至少一种：触摸屏、语音交互装置、多个按键、

- 15 滑动开关（或具有至少两个选择的交互控件）；以及

保护模块，连接在所述第一端口和所述第二端口之间，用于实现上述实施例提供的数据安全保护方法中的步骤。

本申请还一实施例提供一种设备系统，该系统包括：计算机设备，存储设备以及上述实施例提供的中间设备。

- 20 本申请还一实施例提供一种存储设备，该存储设备包括：

第一端口，用于连接计算机设备；

保护芯片，用于实现上述实施例提供的所述数据安全保护方法中的步骤；

控制芯片，通过所述保护芯片与所述第一端口连接；

存储芯片，与所述控制芯片连接，用于在所述控制芯片的控制下，对存

- 25 储空间内的数据进行存储管理。

本申请还一实施例提供一种存储设备，该存储设备包括：

第一端口，用于连接计算机设备；

控制芯片，其上部署有保护模块，用于实现上述实施例提供的所述数据安全保护方法中的步骤；

存储芯片，通过所述控制芯片与所述第一端口连接，用于在所述控制芯片的控制下，对存储空间内的数据进行存储管理。

5 本申请又一实施例提供了一种存储设备。该存储设备包括：

第一端口，用于连接计算机设备；

控制芯片，与第一端口连接，用于基于所述计算机设备发送的数据交互指令，生成相应的控制指令；

存储芯片，与所述控制芯片连接；

10 其中，所述存储芯片上部署有保护模块，用于采用上述实施例所述数据安全保护方法中的步骤，处理所述控制芯片发送的控制指令。

为了执行上述方法实施例对应的数据安全保护方法，以实现相应的功能和技术效果。参见图 30，图 30 示出了本申请实施例提供的一种数据安全保护模块的结构框图。为了便于说明，仅示出了与本实施例相关的部分，本申请
15 实施例提供的数据安全保护模块，应用于目标设备，所述目标设备设有保护模块，所述保护模块包含至少一种保护模式，所述保护模式用于控制计算机设备在存储设备上的读写权限，所述装置包括：

控制单元 1301，用于根据所述目标设备的当前保护模式，对所述计算机设备发送的数据交互指令进行权限控制，所述数据交互指令用于所述计算机
20 设备与所述存储设备进行数据交互；

响应单元 1302，用于若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应。

在一些实施例中，所述装置还包括：

识别单元，用于若检测到所述计算机设备与所述存储设备之间的通信连接请求，则识别所述第一接口的设备类型；
25

建立单元，用于若所述设备类型为预设允许通信类型，则建立所述计算机设备与所述存储设备之间的通信连接。

在一些实施例中，若所述目标设备为具有保护模块的中间设备，所述中间设备设有用于连接存储设备的第一接口，和用于连接计算机设备的第二接口；所述装置，还包括：

5 第一检测单元，用于当所述第一接口接入所述存储设备，且所述第二接口接入所述计算机设备时，检测所述计算机设备与所述存储设备之间的通信连接请求。

在一些实施例中，所述装置，还包括：

中断单元，用于若所述设备类型为预设禁止通信类型，则中断所述通信连接请求。

10 在一些实施例中，所述建立单元，包括：

发送子单元，用于将所述存储设备的目标硬件特征参数发送至所述计算机设备，所述目标硬件特征参数用于建立所述计算机设备与所述存储设备之间的通信连接。

在一些实施例中，所述发送子单元，具体用于：

15 根据所述存储设备的设备类型，从预设的参数模板中，获取与所述设备类型对应的目标硬件特征参数。

将所述目标硬件特征参数发送至所述计算机设备。

在一些实施例中，所述发送子单元，具体还用于：

获取所述存储设备的硬件特征参数；

20 根据预设的参数类型，对所述硬件特征参数进行筛选，以确定与所述参数类型对应的目标硬件特征参数；

将所述目标硬件特征参数发送至所述计算机。

在一些实施例中，所述控制单元 1301，包括：

识别子单元，用于识别所述数据交互指令的指令类型；

25 判定子单元，用于若所述指令类型为所述权限要求对应的预设指令类型，则判定所述数据交互指令满足所述当前保护模式对应的权限要求。

在一些实施例中，所述保护模式为只读模式，所述装置还包括：

返回单元，用于响应于所述计算机设备发送的参数读取请求，将只读参数返回至所述计算机设备，所述只读参数用于使所述计算机设备将所述存储设备识别为只读设备。

在一些实施例中，所述响应单元 1302，包括：

- 5 响应子单元，用于响应于所述数据交互指令，对所述存储设备中的目标文件进行读写操作，所述读写操作包括读操作和写操作中的至少一种。

在一些实施例中，若所述保护模式为全盘只读模式，所述响应子单元，具体用于：

- 10 响应于所述数据交互指令，向所述计算机设备反馈第三目标数据，所述数据交互指令为读取指令，所述第三目标数据为所述存储设备响应于所述读取指令返回的数据。

在一些实施例中，若所述保护模式为特定文件读写模式，所述响应子单元，具体用于：

- 15 响应于所述数据交互指令，将所述目标文件的扇区地址映射至目标地址，所述目标文件为显示于所述计算机设备的文件；

基于所述目标地址，对所述目标文件进行读写操作。

在一些实施例中，所述目标文件包括所述存储设备已有的特定文件或预设文件，或者在所述计算机设备与所述存储设备建立通信连接前自动生成的文件。

- 20 在一些实施例中，若所述保护模式为限位读写模式，所述响应子单元，具体用于：

响应于所述数据交互指令，基于预设扇区地址区间，对所述数据交互指令对应的目标扇区地址进行验证，所述目标扇区地址为所述存储设备基于所述数据交互指令执行读写操作时的扇区地址；

- 25 若所述目标扇区地址在所述预设扇区地址区间内，则在所述存储设备的目标扇区地址进行读写操作。

在一些实施例中，在所述保护模式为文件限制读写模式时，所述响应子

单元，具体用于：

响应于所述数据交互指令，基于预设文件特征，对所述数据交互指令对应的目标文件特征进行验证，所述目标文件特征为所述存储设备基于所述数据交互指令执行读写操作时对应的文件特征；

- 5 若所述目标文件特征符合所述预设文件特征，则对所述存储设备中的所述目标文件进行读写操作。

在一些实施例中，所述响应子单元，具体还用于：

若所述目标文件特征不符合所述预设文件特征，则对所述目标文件进行隐藏。

- 10 在一些实施例中，所述预设文件特征包括文件中预设扇区数据对应的第一哈希值；响应子单元，具体还用于：

计算所述目标文件中预设扇区数据的第二哈希值；

若所述第二哈希值与所述第一哈希值一致，则判定所述目标文件特征符合所述预设文件特征；

- 15 若所述第二哈希值与所述第一哈希值不一致，则判定所述目标文件特征不符合所述预设文件特征。

在一些实施例中，若保护模式为加密写入模式，所述响应子单元，具体用于：

- 20 响应于所述数据交互指令，对所述数据交互指令携带的待写入数据进行加密处理，得到第一目标数据；

向所述存储设备中的所述目标文件写入所述第一目标数据。

在一些实施例中，若保护模式为解密读取模式，所述响应子单元，具体用于：

- 25 响应于所述数据交互指令，向所述计算机设备反馈第二目标数据，所述第二目标数据为对所述存储设备响应于所述数据交互指令返回的数据进行解密后的数据。

在一些实施例中，若所述保护模式为人工确认模式，所述响应子单元，

具体用于：

响应于所述数据交互指令，提示用户是否确认执行所述数据交互指令；

若接收到所述数据交互指令的确认执行指令，则对所述存储设备中的目标文件进行读写操作。

5 在一些实施例中，所述响应子单元，具体还用于：

基于预设读写规则，对所述读写操作进行异常验证；

若所述读写操作不符合所述预设读写规则，则判定所述读写操作异常。

在一些实施例中，所述装置还包括：

10 第一接入单元，用于将目标扇区区间作为存储数据源接入到所述计算机设备，所述目标扇区区间通过切割所述存储设备的存储空间得到，所述存储数据源包含所述目标文件。

在一些实施例中，所述装置还包括：

第一读取单元，用于读取所述存储设备的扇区信息；

15 切割单元，用于基于所述扇区信息，切割所述存储设备的存储空间，得到所述存储设备对应的多个扇区区间，所述目标扇区区间为多个所述扇区区间中的至少一个。

在一些实施例中，所述装置还包括：

第二接入单元，用于将镜像文件作为所述存储数据源接入到所述计算机设备，所述镜像文件基于预设镜像策略生成得到。

20 在一些实施例中，所述存储设备为联网存储设备，所述联网存储设备与服务端连接，所述服务端包含多个联网镜像文件，所述装置还包括：

第三接入单元，用于将目标联网镜像文件作为存储数据源接入到所述计算机设备，所述目标联网镜像文件为多个所述联网镜像文件中的至少一个，所述存储数据源包含所述目标文件。

25 所述装置还包括：

验证单元，用于响应于用户输入的验证指令，将与所述验证指令的指令类型对应的目标存储数据源接入到所述计算机设备，所述目标存储数据源为

扇区区间、镜像文件和联网镜像文件中的至少一种。

在一些实施例中，所述装置还包括：

第二读取单元，用于读取所述存储设备的用电需求信息；

配置单元，用于根据所述用电需求信息，配置所述存储设备的电路保护策略，所述电路保护策略用于控制所述存储设备的用电状态。

在一些实施例中，所述装置还包括：

生成单元，用于生成交互日志，所述日志用于记录对于所述计算机发送的数据交互指令的处理记录。

上述的数据安全保护模块可实施上述方法实施例的数据安全保护方法。

上述方法实施例中的可选项也适用于本实施例，这里不再详述。本申请实施例的其余内容可参照上述方法实施例的内容，在本实施例中，不再进行赘述。

图 31 为本申请一实施例提供的目标设备的结构示意图。如图 31 所示，该实施例的目标设备 14 包括：至少一个处理器 140（图 14 中仅示出一个）处理器、存储器 141 以及存储在所述存储器 141 中并可在所述至少一个处理器 140 上运行的计算机程序 142，所述处理器 140 执行所述计算机程序 142 时实现上述任意方法实施例中的步骤。

所述目标设备 14 可以是具有保护模块的中间设备或存储设备。该目标设备可包括但不限于处理器 140、存储器 141。本领域技术人员可以理解，图 31 仅仅是目标设备 14 的举例，并不构成对目标设备 14 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，例如还可以包括输入输出设备、网络接入设备等。

所述处理器 140 可以是中央处理单元(Central Processing Unit, CPU)，该处理器 140 还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor, DSP)、专用集成电路 (Application Specific Integrated Circuit, ASIC)、现成可编程门阵列 (Field-Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

所述存储器 141 在一些实施例中可以是所述目标设备 14 的内部存储单元, 例如目标设备 14 的硬盘或内存。所述存储器 141 在另一些实施例中也可以是所述目标设备 14 的外部存储设备, 例如所述目标设备 14 上配备的插接式硬盘, 智能存储卡 (Smart Media Card, SMC), 安全数字 (Secure Digital, SD) 卡, 闪存卡 (Flash Card) 等。进一步地, 所述存储器 141 还可以既包括所述目标设备 14 的内部存储单元也包括外部存储设备。所述存储器 141 用于存储操作系统、应用程序、引导装载程序(BootLoader)、数据以及其他程序等, 例如所述计算机程序的程序代码等。所述存储器 141 还可以用于暂时地存储已经输出或者将要输出的数据。

- 10 另外, 本申请实施例还提供一种计算机可读存储介质, 所述计算机可读存储介质存储有计算机程序, 所述计算机程序被处理器执行时实现上述任意方法实施例中的步骤。

本申请实施例提供了一种计算机程序产品, 当计算机程序产品在目标设备上运行时, 使得目标设备执行时实现上述各个方法实施例中的步骤。

- 15 在本申请所提供的几个实施例中, 可以理解的是, 流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分, 所述模块、程序段或代码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。也应当注意的是, 在有些作为替换的实现方式中, 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。

- 20 所述功能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, 可以存储在一个计算机可读取存储介质中。基于这样的理解, 本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来, 该计算机软件产品存储在一个存储介质中, 包括若干指令用以使得一台目标设备执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括: U 盘、移动硬盘、只读存储器 (ROM, Read-Only Memory)、随机存取存储器 (RAM, Random Access Memory)、

(硬盘、SD 卡、TF 卡、) 磁碟或者光盘等各种可以存储程序代码的介质。

以上所述的具体实施例，对本申请的目的、技术方案和有益效果进行了进一步的详细说明，应当理解，以上所述仅为本申请的具体实施例而已，并不用于限定本申请的保护范围。特别指出，对于本领域技术人员来说，凡在
5 本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

1、一种数据安全保护方法，其特征在于，应用于保护模块，所述保护模块包含至少一种保护模式，所述保护模式用于对计算机设备与存储设备间的交互进行控制，以对所述计算机设备及所述存储设备进行安全性保护；所述方法包括：

根据所述保护模块的当前保护模式，对所述计算机设备发送的数据交互指令进行权限控制，所述数据交互指令用于所述计算机设备与所述存储设备进行数据交互；

若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应；

其中，所述保护模块设置在所述计算机设备的用于连接存储设备的接口，或所述存储设备上，或中间设备上；所述中间设备连接所述计算机设备与所述存储设备。

2、根据权利要求1所述的方法，其特征在于，若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应，包括：

所述数据交互指令针对的数据源是所述当前保护模式指定的至少一个数据源中的一个，且所述数据交互指令对所述数据源内数据的操作类型符合所述当前保护模式规定的操作类型时，对所述数据交互指令做出响应。

3、根据权利要求2所述的方法，其特征在于，所述保护模块设置在第一存储设备上，且第一存储设备上设有至少一个或多个存储芯片以及用于连接至少一个或多个外部第二存储设备的接口，所述第一存储设备上的至少部分接口连接有外部第二存储设备；

所述当前保护模式指定的至少一个数据源包括：

所述至少一个或多个存储芯片、所述第一存储设备上至少部分接口连接的外部第二存储设备中的至少一个物理数据源；和/或

所述至少一个或多个存储芯片中的至少一个逻辑分盘；和/或

所述第一存储设备上连接的外部第二存储设备中的至少一个逻辑分盘。

4、根据权利要求1所述的方法，其特征在于，所述计算机设备与所述保护模块间的交互过程包括：准备阶段、枚举阶段和数据交换阶段；

根据所述保护模块的当前保护模式，对所述计算机设备发送的数据交互指令进行权限控制，若所述数据交互指令满足所述当前保护模式对应的权限

5 要求，对所述数据交互指令做出响应，为所述数据交互阶段中的步骤。

5、根据权利要求4所述的方法，其特征在于，

所述保护模块设置在中间设备上时，所述方法还包括：在准备阶段，所述中间设备读取所述存储设备的数据信息并分析；

所述保护模块设置在存储设备上时，所述方法还包括：在准备阶段，所述保护模块对所述存储设备的数据信息进行分析；

其中，所述数据信息包括如下中的至少一项：存储设备的第一特征参数、存储设备的第一存储信息相关参数及地址信息。

6、根据权利要求5所述的方法，其特征在于，所述当前保护模式为特定文件模式时，所述地址信息包括：根目录首扇区地址、至少一个特定文件或文件夹的首扇区地址。

7、根据权利要求5所述的方法，其特征在于，还包括：

响应于计算机设备的供电信号，进入所述准备阶段；

在准备阶段，所述中间设备读取所述存储设备的数据信息，包括：

在所述准备阶段，所述中间设备模拟所述计算机设备向所述中间设备发送控制指令；

接收所述存储设备反馈的所述存储设备的数据信息。

8、根据权利要求5所述的方法，其特征在于，对所述数据信息进行分析，包括：

基于所述数据信息，判定存储设备是否是所述当前保护模式指定的设备类型；

若是，则向计算机设备发送枚举信号，以进入枚举阶段。

9、根据权利要求4所述的方法，其特征在于，还包括：

在枚举阶段，基于当前保护模式，对所述存储设备的数据信息进行处理，得到处理后信息；

将处理后信息发送至所述计算机设备，以便建立所述计算机设备与存储设备间的通信连接。

- 5 10、根据权利要求 9 所述的方法，其特征在于，基于当前保护模式，对所述存储设备的数据信息进行处理，得到处理后信息，包括：

根据当前保护模式，对所述数据信息进行处理，生成模拟所述存储设备的第二特征参数；和/或

- 10 根据当前保护模式，对所述数据信息进行处理，生成模拟所述存储设备的第二存储信息相关参数；

将所述第二特征参数和/或所述第二存储信息相关参数发送至所述计算机设备，以便建立所述计算机设备与所述存储设备间的通信连接。

11、根据权利要求 10 所述的方法，其特征在于，根据当前保护模式，对所述数据信息进行处理，生成模拟所述存储设备的第二特征参数，包括：

- 15 获取所述当前保护模式对应的预设参数模板；根据所述数据信息中的第一特征参数反映出的所述存储设备的设备类型，从所述预设参数模板中获取能表征所述设备类型设备的至少一个参数项，以得到所述第二特征参数；或者

- 20 利用所述当前保护模式对应的筛选策略，对所述第一特征参数中的参数项进行筛选，基于筛选出的至少一个参数项作，得到所述第二特征参数。

12、根据权利要求 11 所述的方法，其特征在于，所述第一特征参数包括：描述符数据；其中，描述符数据包括如下中的至少一项：硬件描述符、接口描述符、端口描述符、端点描述符、字符串描述符。

- 25 13、根据权利要求 10 所述的方法，其特征在于，所述数据信息包括第一存储信息相关参数，所述第一存储信息相关参数包括如下中的至少一项：存储设备可读写状态、可格式化块总数、最后逻辑块地址、单扇区字节数、最大逻辑单元数、设备信息。

14、根据权利要求 13 所述的方法，其特征在于，根据当前保护模式，对所述数据信息进行处理，生成模拟所述存储设备的第二存储信息相关参数，包括：

根据当前保护模式规定的操作类型，修改所述第一存储信息相关参数中的
5 的读写状态参数；

若所述当前保护模式为逻辑分盘模式，则根据当前保护模式规定的可接入计算机设备的目标分盘的参数，修改所述第一存储信息相关参数中的可格式化块总数和/或最后逻辑块地址；

根据当前保护模式，修改所述第一存储信息相关参数中的设备信息，以
10 保护存储设备的隐私信息。

15、根据权利要求 8 所述的方法，其特征在于，还包括：

基于所述数据信息判定所述存储设备不是所述当前保护模式指定的设备类型时，终止与所述存储设备的通信；

向所述计算机设备发送第一信息，以便所述计算机设备基于所述第一信息
15 显示虚拟盘标识和/或非正常设备提示信息；

其中，若显示有虚拟盘标识，所述第一信息还包含有所述第一特征参数对应的文本，所述文本在所述虚拟盘标识对应的根文件夹中保存。

16、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，对所述数据交互指令做出响应，包括：

20 根据所述数据交互指令，按照地址映射规则，确定目标地址；

获取目标地址的数据；

按照预设的内容修改规则，对所述目标地址的数据进行数据修改；

将修改后的所述数据，反馈至所述计算机设备。

17、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，还包括：

25 响应于用户在所述第一设备的交互装置上的操作，获取用户在所述至少一个保护模式中选出的目标保护模式；

将所述目标保护模式作为所述保护模块的当前保护模式；

其中，所述交互装置包括如下中的至少一种：触摸屏、语音交互装置、多个按键、滑动开关、具有至少两个选择的交互控件。

18、根据权利要求 17 所述的方法，其特征在于，所述至少一个保护模式包括如下中的至少一个：

5 只读模式，所述只读模式指定的数据源为存储设备的全盘数据，规定的操作类型为只读类型；

 特定文件模式，所述特定文件模式指定的数据源为存储设备中的至少一个特定文件，规定的操作类型为读类型、或写类型、或读写类型；

 空白文件模式，所述空白文件模式指定的数据源为存储设备中自动创建
10 和/或人工创建的至少一个空白文件，规定的操作类型为写类型或读写类型；

 扇区限位模式，所述扇区限位模式指定的数据源为存储设备中的至少一个特定扇区区间，规定的操作类型为读类型、或写类型、或读写类型；

 文件类型限制模式，文件类型限制模式指定的数据源为存储设备中的至少一种特定类型的文件，规定的操作类型为读类型，或写类型、或读写类型；

15 加密写入模式，所述加密写入模式指定的数据源为存储设备中的至少一个第一扇区区间内的数据、至少一个第一文件和/或至少一种类型的文件，规定的操作类型为写类型；

 解密读出模式，所述解密读出模式指定的数据源为存储设备中的至少一个第二扇区区间内的数据、至少一个第二文件和/或至少一种类型的文件，规
20 定的操作类型为读类型；

 人工确认模式，所述人工确认模式指定的数据源为存储设备中的至少一个第三扇区区间内的数据、至少一个第三文件和/或至少一种类型的文件，规定的操作类型为读写类型；

 逻辑分盘模式，所述逻辑分盘模式指定的数据源为存储设备中的至少一个分盘，规定的操作类型为读类型，或写类型，或读写类型；
25

 硬件类型接入保护模式，所述硬件类型接入保护模式无指定数据源，在所述硬件类型接入保护模式下判定存储设备是否为指定的设备类型；

存储设备的数据信息保护模式，所述存储设备的数据信息保护模式无指定数据源，在所述存储设备的数据信息保护模式下，对向计算机设备发送的存储设备的数据信息进行保护性处理，在枚举阶段将保护性处理后的存储设备的数据信息发送至所述计算机设备；

- 5 设备隐私保护模式，所述设备隐私保护模式无指定数据源，在所述设备隐私保护模式下，对向计算机设备发送的设备隐私信息进行保护性处理；

备份模式，所述备份模式无指定数据源，在备份模式下，对计算机设备写入的数据同步写入至指定的备份存储区域内，和/或保护模块在执行写入指令之前读取所述计算机设备写入的扇区地址数据并写入至指定的备份存储区域
10 域内，和/或将接入的存储设备的重要数据扇区的数据备份存储至指定的备份存储区域内；若触发还原，则将所述指定的备份存储区域内的数据读出，写入至所述存储设备原有的数据扇区内。

19、根据权利要求 18 所述的方法，其特征在于，还包括：

- 15 当所述当前保护模式为空白文件模式时，创建至少一个空白文件或文件夹。

20、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，还包括：

当所述当前保护模式为特定文件模式时，输出是否设置空白文件或文件夹的提示信息；

- 20 响应于用户针对所述设置空白文件或文件夹的提示信息的确认指令，在所述存储设备中创建一个文件或文件夹，作为所述特定文件模式对应的特定文件或文件夹；

响应于用户针对所述设置空白文件或文件夹的提示信息的否定指令，获取用户指定的至少一个文件或文件夹，将用户指定的至少一个文件或文件夹作为所述特定文件模式对应的特定文件或文件夹。

- 25 21、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，还包括：

当所述当前保护模式为特定文件模式时，确定所述存储设备中的至少一个特定文件或文件夹；

获取所述至少一个特定文件或文件夹的地址信息；

建立所述至少一个特定文件或文件夹的地址信息与根目录地址的映射关系。

22、根据权利要求 21 所述的方法，其特征在于，还包括：

- 5 计算机设备与存储设备建立通信后，接收到所述计算机设备请求读取所述存储设备的根目录地址时，基于所述映射关系，确定与所述根目录地址存在映射关系的至少一个特定文件或文件夹的地址信息，以读取所述地址信息对应的数据或在所述地址信息对应区域写入数据。

- 23、根据权利要求 21 所述的方法，其特征在于，所述至少一个特定文件
10 或文件夹的地址信息包括：

至少一个特定文件或文件夹的首扇区地址或扇区地址集合；或者
文件分配表中至少一个特定文件或文件夹被记录的簇或块信息。

- 24、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，所述当前
保护模式是人工确认模式时，
15 对所述数据交互指令做出响应，包括：

显示所述数据交互指令预写入或读出数据的相关信息；

响应于用户针对所述相关信息触发确认操作，基于所述数据交互指令向
存储设备写入或读取所述数据。

- 25、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，所述当前
20 保护模式为备份模式时，对所述数据交互指令进行响应，包括：

所述数据交互指令为写指令时，将所述计算机设备写入的数据同步写入
至指定的备份存储区域内；和/或

所述数据交互指令为写指令时，保护模块在执行写入指令前，读取所述
计算机设备写入的扇区地址数据并写入至指定的备份存储区域内。

- 25 26、根据权利要求 25 所述的方法，其特征在于，所述当前保护模式为备
份模式时，所述方法还包括：

将接入存储设备的重要数据扇区的数据备份存储至指定的备份存储区域

内；

当触发还原时，将所述指定的备份存储区域内的数据读出，写入至所述存储设备原有的数据扇区内。

- 27、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，对所述数据交互指令做出响应，包括：

获取所述存储设备基于所述数据交互指令读取数据和/或写入数据的过程信息；

基于过程信息，确定是否存在异常；

若存在异常，则向存储设备发送停止指令。

- 10 28、根据权利要求 27 所述的方法，其特征在于，基于过程信息，确定是否存在异常，包括如下中的至少一项：

若所述存储设备基于所述数据交互指令读取数据的过程不符合设定过程规律，则确定存在异常；

- 15 若所述存储设备基于所述数据交互指令读取数据和/或写入数据的过程没有指定上下文操作，则确定存在异常；其中，读取数据时，指定上下文操作为读取该数据所在文件夹的操作；写入数据时，指定上下文操作为获取所述数据所在文件夹的操作；

若所述存储设备基于所述数据交互指令读取数据和/或写入数据的过程没有从所述数据所在簇或块的首地址开始读或写操作，则确定存在异常；

- 20 若所述存储设备基于所述数据交互指令在预设时长内读取了超过设定数量个文件，则确定存在异常。

29、根据权利要求 27 所述的方法，其特征在于，还包括：

若存在异常，则向计算机设备发送反馈信息；其中，所述反馈信息包括：模拟写入成功的虚假信息，或将预设数据作为成功从存储设备读取的数据；

- 25 和/或

若存在异常，则输出人工确认提示信息，以便用户基于所述人工确认提示信息确定是否继续执行。

30、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，还包括：

若用户选出的当前保护模式为逻辑分盘模式，则对所述存储设备的特定存储空间进行划分，得到至少一个分盘；

5 从所述至少一个分盘中选定一个分盘作为目标分盘，接入所述计算机设备。

31、根据权利要求 30 所述的方法，其特征在于，还包括如下中至少一个步骤：

响应于用户的设置，确定所述特定存储空间；所述特定存储空间为存储设备的全部或部分空间；

10 基于所述逻辑分盘模式中特定存储空间的选定规则，确定所述特定存储空间。

32、根据权利要求 30 所述的方法，其特征在于，对所述存储设备的特定存储空间进行划分，得到至少一个分盘，包括：

15 响应于用户的划分指令，读取所述特定存储空间的扇区信息，基于所述扇区信息，对所述特定存储空间进行划分；或者

读取所述特定存储空间的扇区信息，基于所述扇区信息并利用预置的划分策略，对所述特定存储空间进行划分；或者

在存储设备的文件系统中，生成至少一个镜像文件，以所述至少一个镜像文件分别对应的地址区间，对所述存储设备的特定存储空间进行划分。

20 33、根据权利要求 32 所述的方法，其特征在于，还包括：

在本地获取所述预置分盘策略；或者

从网络侧服务端，获取所述预置分盘策略。

34、根据权利要求 30 所述的方法，其特征在于，从所述至少一个分盘中选定一个分盘作为目标分盘，包括：

25 响应于用户通过交互装置对所述至少一个分盘的选择操作，将用户选定的一个分盘作为目标分盘；或者

接收到指定设备发送的分盘选择指令时，将所述分盘选择指令指示的分

盘作为目标分盘；其中，指定设备通过近场通信或远程通信方式与保护模块通信；其中，所述指定设备与所述计算机设备为不同的设备；或者

接收计算机设备发送的携带有盘密钥的信息，对所述盘密钥进行验证，验证通过后，将所述至少一个分盘中具有该盘密钥的分盘作为目标分盘。

- 5 35、根据权利要求 1 至 15 中任一项所述的方法，其特征在于，所述保护模块设置在所述中间设备上；所述中间设备具有联网功能，以连接云端或服务端侧的存储模块；以及

对所述数据交互指令做出响应，包括：

- 10 将所述数据交互指令发送至网络侧存储模块，以便所述存储模块基于所述数据交互指令读取和/或写入相应的数据。

36、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，在所述保护模式为文件类型限制模式时，对所述数据交互指令做出响应，包括：

- 15 响应于所述数据交互指令，基于预设文件特征，对所述数据交互指令对应的目标文件特征进行验证，所述目标文件特征为所述存储设备基于所述数据交互指令执行读和/或写操作时对应的文件特征，所述文件特征与文件类型相关；

若所述目标文件特征符合所述预设文件特征，则对所述存储设备中的所述目标文件进行读和/或写操作。

- 20 37、根据权利要求 36 所述的数据安全保护方法，其特征在于，对所述数据交互指令对应的目标文件特征进行验证之后，还包括：

若所述目标文件特征不符合所述预设文件特征，则对所述目标文件进行隐藏。

- 25 38、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，若保护模式为加密写入模式，对所述数据交互指令做出响应，包括：

响应于所述数据交互指令，对所述数据交互指令携带的待写入数据进行加密处理，得到第一目标数据；

向所述存储设备中的目标文件写入所述第一目标数据。

39、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，若保护模式为解密读取模式，对所述数据交互指令做出响应，包括：

响应于所述数据交互指令，向所述计算机设备反馈第二目标数据，所述
5 第二目标数据为对所述存储设备响应于所述数据交互指令返回的数据进行解密后的数据。

40、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，所述若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应之前，还包括：

10 将镜像文件作为所述存储数据源接入到所述计算机设备，所述镜像文件基于预设镜像策略生成得到。

41、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，所述存储设备为联网存储设备，所述联网存储设备与服务端连接，所述服务端包含多个联网镜像文件，所述若所述数据交互指令满足所述当前保护
15 模式对应的权限要求，对所述数据交互指令做出响应之前，还包括：

将目标联网镜像文件作为存储数据源接入到所述计算机设备，所述目标联网镜像文件为多个所述联网镜像文件中的至少一个。

42、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，所述方法还包括：

20 响应于用户输入的验证指令，将与所述验证指令的指令类型对应的目标存储数据源接入到所述计算机设备，所述目标存储数据源为扇区区间、镜像文件和联网镜像文件中的至少一种。

43、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应，包括：
25

所述数据交互指令满足所述当前保护模式对应的权限要求，且所述数据交互指令为读取或修改文件内容数据时，确定扇区地址，读取或写入存储设

备对应扇区的数据并返回；

所述方法还包括：所述数据交互指令不满足所述当前保护模式对应的权限要求时，返回错误的状态响应、或返回执行成功响应、或响应空白数据、或将预设数据作为反馈数据进行响应。

- 5 44、根据权利要求 1 至 15 中任一项所述的数据安全保护方法，其特征在于，若所述数据交互指令满足所述当前保护模式对应的权限要求，对所述数据交互指令做出响应，包括：

所述数据交互指令满足所述当前保护模式对应的权限要求，且所述数据交互指令为创建新文件、删除文件或修改文件时，

- 10 确定扇区地址；

若所述数据交互指令包含多个文件的信息，所述存储设备对应的所述扇区地址含有所述多个文件中的部分文件，则确定所述计算机设备要在所述扇区地址创建至少一个文件，基于当前保护模式判定是否允许创建所述至少一个文件或触发与所述当前保护模式组合在一起的其他保护模式；其中，创建

15 的至少一个文件为所述多个文件中除已有的部分文件之外的剩余文件；

- 若所述数据交互指令包含多个文件的信息，且所述多个文件中至少部分文件带有删除标记，则查找所述存储设备对应所述扇区地址内与所述多个文件中带有删除标记的部分文件关联的至少一个预删除文件；确定所述计算机设备要将所述至少一个预删除文件删除，基于当前保护模式判定是否允许创
- 20 建删除所述至少一个预删除文件或触发与所述当前保护模式组合在一起的其他保护模式；

- 若所述数据交互指令包含第一文件集合，所述存储设备对应的所述扇区地址含有第二文件集合，且所述第一文件集合为所述第二文件集合的子集，则确定所述计算机设备要将所述第二文件集合中不属于所述第一文件集合的
- 25 至少一个文件删除，基于当前保护模式判定是否允许删除或触发与所述当前保护模式组合在一起的其他保护模式；

若所述数据交互指令包含的第一文件的除文件名外的属性信息与所述存

储设备对应的所述扇区地址内的第二文件的除文件名外的属性信息相同，则确定所述计算机设备要将所述扇区地址内的所述第二文件的文件名修改为所述第一文件的文件名；基于当前保护模式判定是否允许修改文件名或触发与所述当前保护模式组合在一起的其他保护模式；

- 5 若所述数据交互指令包含的第一文件的文件名与所述存储设备对应扇区地址内的第二文件的文件名相同，且所述第一文件的除文件名外的属性信息与所述第二文件的除文件名外的属性信息不同，则确定所述计算机设备要将所述第二文件的除文件名外的属性信息修改为所述第一文件的除文件名外的属性信息，基于当前保护模式判定是否允许修改属性信息或触发与所述当前
- 10 保护模式组合在一起的其他保护模式。

45、一种中间设备，其特征在于，包括：

第一端口，用于连接计算机设备；

第二端口，用于连接存储设备；

- 15 交互模块，包括如下中的至少一种：触摸屏、语音交互装置、多个按键、滑动开关、具有至少两个选择的交互控件；以及

保护模块，连接在所述第一端口和所述第二端口之间，用于实现上述权利要求 1~44 中任一项所述数据安全保护方法中的步骤。

46、根据权利要求 45 所述的中间设备，其特征在于，还包括：

- 20 通信组件，与所述保护模块连接，用于联网，以将保护模块与云端或服务端侧的存储模块连接，在对所述数据交互指令做出响应时，将所述数据交互指令发送至网络侧存储模块，以便所述存储模块基于所述数据交互指令读取和/或写入相应的数据。

- 25 47、一种设备系统，其特征在于，包括：

计算机设备；

存储设备；以及

上述权利要求 45 或 46 所述的中间设备。

48、一种存储设备，其特征在于，包括：

第一端口，用于连接计算机设备；

保护芯片，用于实现上述权利要求 1~44 中任一项所述数据安全保护方法

5 中的步骤；

控制芯片，通过所述保护芯片与所述第一端口连接；

存储芯片，与所述控制芯片连接，用于在所述控制芯片的控制下，对存储空间内的数据进行存储管理。

10 49、一种存储设备，其特征在于，包括：

第一端口，用于连接计算机设备；

控制芯片，其上部署有保护模块，用于实现上述权利要求 1~44 中任一项所述数据安全保护方法中的步骤；

15 存储芯片，通过所述控制芯片与所述第一端口连接，用于在所述控制芯片的控制下，对存储空间内的数据进行存储管理。

50、一种存储设备，其特征在于，包括：

第一端口，用于连接计算机设备；

20 控制芯片，与第一端口连接，用于基于所述计算机设备发送的数据交互指令，生成相应的控制指令；

存储芯片，与所述控制芯片连接；

其中，所述存储芯片上部署有保护模块，用于采用上述权利要求 1~44 中任一项所述数据安全保护方法中的步骤，处理所述控制芯片发送的控制指令。

25 51、一种安全控制框架，其特征在于，所述安全控制框架包括：

配置模块，用于配置保护场景；

生成模块，用于生成保护场景的配置信息或带有所述保护场景的软件；

其中，一种保护场景对应至少一种保护模式；将所述配置信息或带有所述保护场景的软件部署在硬件设备上，使得所述硬件设备具有上述权利要求1~44中任一项所述数据安全保护方法中的步骤对应的功能。

52、根据权利要求51所述的安全控制框架，其特征在于，配置模块在配置保护场景时，具体用于：

配置保护场景标识信息；

配置所述保护场景对应的保护操作的策略。

53、根据权利要求52所述的安全控制框架，其特征在于，配置所述保护场景对应的保护操作的策略，包括以下至少一项：

10 配置所述保护场景下准备阶段内保护操作的策略；

配置所述保护场景下枚举阶段内保护操作的策略；

配置所述保护场景下数据交互阶段内保护操作的策略。

54、根据权利要求51~53中任一项所述的安全控制框架，其特征在于，还包括：

15 编译模块，用于根据所述配置信息执行相应的软件编译策略得到安全控制软件；

其中，硬件设备运行该安全控制软件，使得硬件设备具有上述权利要求1~44中任一项所述数据安全保护方法中的步骤对应的功能。

20 55、一种计算机可读存储介质，其特征在于，其存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至44中任一项所述数据安全保护方法的步骤。