(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104808951 B
(45)授权公告日 2018.02.09

(21)申请号 201410042329.4

(22)申请日 2014.01.28

(65)同一申请的已公布的文献号
申请公布号 CN 104808951 A

(43)申请公布日 2015.07.29

(73)专利权人 国际商业机器公司
地址 美国纽约阿芒克

(72)发明人 苏芊 尤薇 孙宇 石永红

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 酆迅 李峥宇

(51)Int.Cl.
G06F 3/06(2006.01)

(56)对比文件
CN 102473216 A,2012.05.23,
CN 103049534 A,2013.04.17,
US 2009132424 A1,2009.05.21,
US 2006288425 A1,2006.12.21,
CN 101827102 A,2010.09.08,

审查员 周静奇

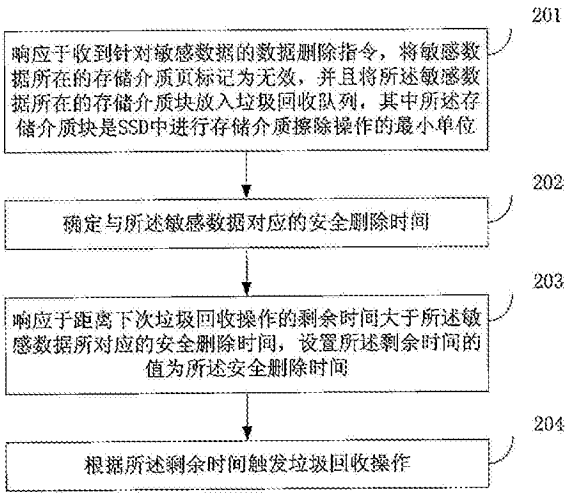
权利要求书2页 说明书10页 附图3页

(54)发明名称

进行存储控制的方法和设备

(57)摘要

本发明实施例提供了用于进行存储控制的方法和设备。所述方法包括:响应于收到针对敏感数据的数据删除指令,将敏感数据所在的存储介质页标记为无效,并且将所述存储介质页所在的存储介质块放入垃圾回收队列,其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位;确定与所述敏感数据对应的安全删除时间;响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间,设置所述剩余时间的值为所述安全删除时间;和根据所述剩余时间触发垃圾回收操作。采用根据本发明实施例的方案可以增强SSD的安全性。



CN 104808951 B

1.一种进行存储控制的方法，该方法包括：

响应于收到针对敏感数据的数据删除指令，将敏感数据所在的存储介质页标记为无效，并且将所述存储介质页所在的存储介质块放入垃圾回收队列，其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位；

确定与所述敏感数据对应的安全删除时间，所述安全删除时间指示所述敏感数据被删除和被擦除之间的最大时间间隔；

响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间，设置所述剩余时间的值为所述安全删除时间；和

根据所述剩余时间触发垃圾回收操作。

2.如权利要求1所述的方法，进一步包括：

接收数据写入指令，所述数据写入指令包括数据，并且所述数据写入指令指示所述数据是否为敏感数据；和

响应于所述数据是敏感数据，将所述数据存储在专用于存储敏感数据的存储介质块中，

其中，所述专用于存储敏感数据的存储介质块不包括有效的用于存储非敏感数据的存储介质页。

3.如权利要求1或2所述的方法，其中所述安全删除时间在删除所述敏感数据时设置。

4.如权利要求1或2所述的方法，其中所述安全删除时间在写入所述敏感数据时设置。

5.如权利要求1或2所述的方法，其中采用不同的模块分别处理敏感数据和非敏感数据。

6.一种进行存储控制的装置，该装置包括：

存储介质块处理模块，配置为响应于收到针对敏感数据的数据删除指令，将敏感数据所在的存储介质页标记为无效，并且将所述存储介质页所在的存储介质块放入垃圾回收队列，其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位；

安全删除时间确定模块，配置为确定与所述敏感数据对应的安全删除时间，所述安全删除时间指示所述敏感数据被删除和被擦除之间的最大时间间隔；

剩余时间设置模块，配置为响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间，设置所述剩余时间的值为所述安全删除时间；和

触发模块，配置为根据所述剩余时间触发垃圾回收操作。

7.如权利要求6所述的装置，进一步包括：

写入指令接收模块，配置为接收数据写入指令，所述数据写入指令包括数据，并且所述数据写入指令指示所述数据是否为敏感数据；和

数据存储模块，配置为响应于所述数据是敏感数据，将所述数据存储在专用于存储敏感数据的存储介质块中，

其中，所述专用于存储敏感数据的存储介质块不包括有效的用于存储非敏感数据的存储介质页。

8.如权利要求6或7所述的装置，其中所述安全删除时间在删除所述敏感数据时设置。

9.如权利要求6或7所述的装置，其中所述安全删除时间在写入所述敏感数据时设置。

10.如权利要求6或7所述的装置，其中采用不同的模块分别处理敏感数据和非敏感数

据。

进行存储控制的方法和设备

■技术领域

[0001] 本发明涉及计算机技术，更具体地说，涉及进行存储控制的方法和设备。

■背景技术

[0002] 在传统的硬盘驱动器(HDD)中，数据的逻辑地址和物理地址具有一一对应的关系。这里，逻辑地址指的是操作系统所处理的地址，而物理地址指的是存储介质上具体的位置。物理地址对操作系统是透明的，由HDD的控制器负责逻辑地址与物理地址的对应。在使用HDD的场合，每次操作系统向同一个逻辑地址写入数据，该数据会被写入到存储介质上的同一个位置。对于数据删除(deletion)而言，一般情况下操作系统会将待删除数据所对应的逻辑地址标注为空闲，从而使得该逻辑地址可以被后续写入操作所使用。在实际发生所述后续写入操作之前，所述待删除数据并没有从存储介质上擦除(erasure)，从而可以通过技术手段读取并恢复。

[0003] 对于某些对安全性要求高的敏感数据，操作系统的删除操作必须是所谓的“安全删除”，即该数据被彻底地从存储介质上擦除。操作系统可以在将所述逻辑地址标注为空闲后立即执行后续写入操作，例如向该逻辑地址写入伪数据(pseudo data)。由于逻辑地址和物理地址是一一对应的，因此在存储所述敏感数据的物理地址上，所述待删除数据被所述伪数据替代，从而无法被读取并恢复。

[0004] 与传统的硬盘驱动器(HDD)相比，基于闪存技术的固态硬盘(SSD)具有速度快的优势。与HDD不同的是，在SSD中，逻辑地址和物理地址并不是一一对应的。如果向同一个逻辑地址先后两次写入数据，那么这两次写入的数据会被存储在不同的物理地址上。这使得在使用SSD的场合，操作系统并不能通过向存储敏感数据的逻辑地址写入伪数据而将对应的敏感数据从存储介质上擦除。

[0005] 具体而言，在SSD中，在对一个逻辑地址进行第一次写入操作以写入第一数据时，SSD向该逻辑地址分配第一物理地址以存储所述第一数据，从而使得所述逻辑地址对应于第一物理地址。在对该逻辑地址进行第二次写入操作以写入第二数据时，SSD向该逻辑地址分配第二物理地址以存储所述第二数据，而并不是先将第一数据从第一物理地址擦除然后将第二数据写入到第一物理地址。这样，与所述逻辑地址对应的物理地址从第一物理地址变为第二物理地址。这样做的原因是，在SSD中，对存储介质的擦除操作必须以存储介质块(block)为单位进行。所述存储介质块的大小一般为2^20比特。另一方面，操作系统对数据的操作往往是以2^9(512)比特为单位的。假设操作系统向同一逻辑地址先后两次写入512字节的数据，那么所涉及的数据仅仅是一个存储介质块中的很小的一部分数据。显然，为了要修改这一小部分数据而将整个存储介质块的数据擦除，这是不切实际的。

[0006] 由此可见，在使用SSD的场合，即使操作系统在删除某个逻辑地址所存储的敏感数据后，立刻向该逻辑地址写入伪数据，也无法将所述敏感数据从SSD上擦除。伪数据会被存储在与敏感数据不同的物理地址，而敏感数据仍然存储在原来的物理地址。结果是，可以通过技术手段从存储敏感数据的物理地址读取并恢复所述敏感数据。

[0007] 因此，需要一种新的解决方案类增强SSD的安全性。

■发明内容

[0008] 本发明实施例提供了进行存储控制的方法和装置。

[0009] 根据本发明实施例的进行存储控制的方法包括：响应于收到针对敏感数据的数据删除指令，将敏感数据所在的存储介质页标记为无效，并且将所述存储介质页所在的存储介质块放入垃圾回收队列，其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位；确定与所述敏感数据对应的安全删除时间；响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间，设置所述剩余时间的值为所述安全删除时间；和根据所述剩余时间触发垃圾回收操作。

[0010] 根据本发明实施例的进行存储控制的装置包括：存储介质块处理模块，配置为响应于收到针对敏感数据的数据删除指令，将敏感数据所在的存储介质页标记为无效，并且将所述存储介质页所在的存储介质块放入垃圾回收队列，其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位；安全删除时间确定模块，配置为确定与所述敏感数据对应的安全删除时间；剩余时间设置模块，配置为响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间，设置所述剩余时间的值为所述安全删除时间；和触发模块，配置为根据所述剩余时间触发垃圾回收操作。

[0011] 采用根据本发明实施例的方案，可以在可控的时间内，将被删除的敏感数据从SSD的存储介质上擦除，从而提高SSD的安全性。

■附图说明

[0012] 通过结合附图对本公开示例性实施方式进行更详细的描述，本公开的上述以及其它目的、特征和优势将变得更加明显，其中，在本公开示例性实施方式中，相同的参考标号通常代表相同部件。

[0013] 图1是适于用来实现本发明实施方式的示例性计算机系统/服务器12的框图；

[0014] 图2示出根据本发明实施例的进行存储控制的方法的流程图；

[0015] 图3示出根据本发明实施例的进行存储控制的方法的流程图；以及

[0016] 图4示出根据本发明实施例的进行存储控制的装置的方框图。

■具体实施方式

[0017] 下面将参照附图更详细地描述本公开的优选实施方式。虽然附图中显示了本公开的优选实施方式，然而应该理解，可以以各种形式实现本公开而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了使本公开更加透彻和完整，并且能够将本公开的范围完整地传达给本领域的技术人员。

[0018] 所属技术领域的技术人员知道，本发明可以实现为系统、方法或计算机程序产品。因此，本公开可以具体实现为以下形式，即：可以是完全的硬件、也可以是完全的软件(包括固件、驻留软件、微代码等)，还可以是硬件和软件结合的形式，本文一般称为“电路”、“模块”或“系统”。此外，在一些实施例中，本发明还可以实现为在一个或多个计算机可读介质中的计算机程序产品的形式，该计算机可读介质中包含计算机可读的程序代码。

[0019] 可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0020] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括——但不限于——电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0021] 计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0022] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言-诸如Java、Smalltalk、C++，还包括常规的过程式程序设计语言-诸如"C"语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)-连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0023] 下面将参照本发明实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机程序指令实现。这些计算机程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理器，从而生产出一种机器，这些计算机程序指令通过计算机或其它可编程数据处理装置执行，产生了实现流程图和/或框图中的方框中规定的功能/操作的装置。

[0024] 也可以把这些计算机程序指令存储在能使得计算机或其它可编程数据处理装置以特定方式工作的计算机可读介质中，这样，存储在计算机可读介质中的指令就产生出一个包括实现流程图和/或框图中的方框中规定的功能/操作的指令装置(instruction means)的制造品(manufacture)。

[0025] 也可以把计算机程序指令加载到计算机、其它可编程数据处理装置、或其它设备上，使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤，以产生计算机实现的过程，从而使得在计算机或其它可编程装置上执行的指令能够提供实现流程图和/或框图中的方框中规定的功能/操作的过程。

[0026] 图1示出了适于用来实现本发明实施方式的示例性计算机系统/服务器12的框图。图1显示的计算机系统/服务器12仅仅是一个示例，不应对本发明实施例的功能和使用范围

带来任何限制。

[0027] 如图1所示，计算机系统/服务器12以通用计算设备的形式表现。计算机系统/服务器12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储器28，连接不同系统组件(包括系统存储器28和处理单元16)的总线18。

[0028] 总线18表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(ISA)总线，微通道体系结构(MAC)总线，增强型ISA总线、时频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0029] 计算机系统/服务器12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被计算机系统/服务器12访问的可用介质，包括易失性和非易失性介质，可移动的和不可移动的介质。

[0030] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质，例如随机存取存储器(RAM)30和/或高速缓存存储器32。计算机系统/服务器12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例，存储系统34可以用于读写不可移动的、非易失性磁介质(图1未显示，通常称为“硬盘驱动器”)。尽管图1中未示出，可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器，以及对可移动非易失性光盘(例如CD-ROM，DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下，每个驱动器可以通过一个或者多个数据介质接口与总线18相连。存储器28可以包括至少一个程序产品，该程序产品具有一组(例如至少一个)程序模块，这些程序模块被配置以执行本发明各实施例的功能。

[0031] 具有一组(至少一个)程序模块42的程序/实用工具40，可以存储在例如存储器28中，这样的程序模块42包括——但不限于——操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本发明所描述的实施例中的功能和/或方法。

[0032] 计算机系统/服务器12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信，还可与一个或者多个使得用户能与该计算机系统/服务器12交互的设备通信，和/或与使得该计算机系统/服务器12能与一个或多个其它计算设备进行通信的任何设备(例如网卡，调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且，计算机系统/服务器12还可以通过网络适配器20与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图所示，网络适配器20通过总线18与计算机系统/服务器12的其它模块通信。应当明白，尽管图中未示出，可以结合计算机系统/服务器12使用其它硬件和域软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0033] 在下面的描述中，假设SSD分配物理地址的最小单位与操作系统处理数据的最小单位一致，这样大小的存储介质称为存储介质页(page)。由此可见，存储介质页与物理地址具有一一对应的关系。还可以理解，“存储介质页”和“存储介质块”一样，都对应于SSD上物理的存储空间。由于存储介质块的大小通常是2^20比特，而存储介质页的大小通常是2^9比特，因此一个存储介质块可以包括多个存储介质页。为了描述方便，假设敏感数据的大小恰好是一存储介质页。

[0034] 如前所述，如果操作系统对同一逻辑地址先后进行两次写入操作，那么在进行第二次写入操作时，SSD将与所述逻辑地址对应的物理地址从第一物理地址变为第二物理地址，并且将第一物理地址所对应的存储介质页标注为失效(invalid)。在某些情况下，SSD会启动垃圾回收(garbage collection)操作以便回收被标注为失效的存储介质页。在对一个目标块进行垃圾回收操作的过程中，目标块中的未被标注为失效的存储介质页中所存储的数据被转移到其他存储介质块中的新的物理地址；与这些存储介质页对应的逻辑地址被重新映射到新的物理地址；然后这个存储介质块被整体地擦除并且被标注成空闲，从而可以写入新的数据。可以理解，对一个目标块进行垃圾回收操作后，可以释放出相当于该目标块中所有失效存储介质页的空闲存储空间。

[0035] 敏感数据删除在操作系统层面体现为与该敏感数据对应的逻辑地址被标注为空闲，从而后续的写入操作可以使用该逻辑地址；在存储器层面，敏感数据删除体现为与该敏感数据对应的物理地址被标注为失效，从而在一定条件下触发SSD的垃圾回收操作。在垃圾回收操作中，所述敏感数据被从存储介质上擦除。因此，为了确保敏感数据被从存储介质上擦除，可以在删除所述敏感数据后，触发SSD的垃圾回收操作。

[0036] 一般来说，SSD会在可以用于写入新数据的空闲存储空间不足的情况下启动垃圾回收操作，因此可以通过向SSD写入大量伪数据来使得SSD中的空闲存储空间不足，从而触发SSD的垃圾回收操作。

[0037] 根据本发明的一个实施例，可以在删除敏感数据后，反复向所述敏感数据所对应的逻辑地址写入伪数据。每向该逻辑地址进行一次伪地址写入，SSD都会向该逻辑地址分配一个新的物理地址，并且将旧的物理地址标注为失效。由于失效的物理地址所对应的存储介质页在擦除前不能用于存储新的数据，从而不能计入空闲的存储空间。可以预见，反复写入伪数据会造成SSD中的空闲存储空间下降，从而触发SSD的垃圾回收操作。由于敏感数据所在的存储介质页是失效存储介质页，因此如果该失效存储介质页所在的存储介质块被作为垃圾回收操作的目标块，那么敏感数据所在的存储介质页就会被擦除。此外，除最后一次写入伪数据时所新分配的存储介质页之外，其他存储有伪数据的存储介质页在所述垃圾回收操作时也都是失效存储介质页，从而也都应该在垃圾回收操作中被擦除并且被标注为空闲存储空间。

[0038] 根据本发明的另一个实施例，也可以在删除敏感数据后，向SSD一次性地写入大量的伪数据。这同样会造成SSD中的空闲存储空间不足从而触发垃圾回收操作。类似地，在垃圾回收操作中，如果敏感数据所在的存储介质块被作为垃圾回收操作的目标块，那么敏感数据所在的存储介质页就会被擦除。

[0039] 这种做法的好处是可以在操作系统层面实施，从而具有相当大的灵活性。然而，在进行垃圾回收操作时，SSD并不一定会将敏感数据所在的存储介质块作为目标块。因此，为了确保敏感数据所在的存储介质块被作为垃圾回收操作的目标块，需要向SSD写入足够多的伪数据，从而使得所有包含失效存储介质页的存储介质块都至少一次被作为垃圾回收操作的目标块。结果是，基本上每次删除敏感数据，都需要对整个SSD进行一次写入/擦除操作。SSD的写入/擦除次数是有限的。这样会缩短SSD的使用寿命。此外，大量的写入或擦除操作所需要的时间很长，从而影响了SSD的I/O效率。

[0040] 图2示出根据本发明实施例的进行存储控制的方法的流程图。

[0041] 步骤201，响应于收到针对敏感数据的数据删除指令，将敏感数据所在的存储介质页标记为无效，并且将所述敏感数据所在的存储介质块放入垃圾回收队列，其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位。

[0042] 如前所述，垃圾回收操作是SSD中的一个常用操作。已经有很多方案来选择垃圾回收操作的目标块。例如，可以选择包含较多无效存储介质页的存储介质块作为所述目标块，也可以选择较长时间没有进行过擦除操作的存储介质块作为所述目标块。在SSD中，存在至少一个垃圾回收队列，该队列中存放的是至少一个指示符，其指示垃圾回收操作的目标块。各种选择垃圾回收操作目标块的方案将其所选择的存储介质块所对应的指示符放入所述垃圾回收队列中。在SSD进行垃圾回收操作时，其对所述队列中的存储介质块分别进行有效数据转移操作，然后对这些存储介质进行擦除。

[0043] 可以理解，数据删除指令至少包括数据的标识符，例如数据的逻辑地址或物理地址。在根据本发明实施例的方案中，需要对操作系统进行一定的增强，使得操作系统发给SSD的数据删除指令可以指示该数据是否为敏感数据。可以在向操作系统安装SSD的驱动程序时进行所述增强，也可以通过在操作系统中打补丁来进行所述增强。

[0044] 根据本发明实施例，所述数据删除指令可以包括一个标记(flag)。SSD可以根据所述标记的值来判断所述数据是否为敏感数据。根据本发明另一个实施例，可以设置两条不同的数据删除指令。SSD可以根据收到的是哪条数据删除指令来判断所述数据是否为敏感数据。

[0045] 根据本发明的另一个实施例，可以事先在SSD和操作系统之间约定，操作系统在存储敏感数据时，只会使用某一特定范围的逻辑地址。这样，SSD可以根据数据删除指令中所包含的逻辑地址来判断所述数据是否为敏感数据。这样做的好处是不用对所述数据删除指令的格式进行任何修正。

[0046] 根据本发明的再一个实施例，可以在SSD中设置专用于存储敏感数据的存储介质块和专用于存储非敏感数据的存储介质块。前者称为敏感数据存储介质块，后者称为非敏感数据存储介质块。SSD根据所述数据删除请求中的数据标识符，确定要删除的数据位于敏感数据存储介质块中还是位于非敏感数据存储介质块，从而确定要删除的数据是否为敏感数据。

[0047] 关于如何实现敏感数据和非敏感数据存储在不同的存储介质块中，将在下面其他附图进行更为详细地描述。

[0048] 步骤202，确定与所述敏感数据对应的安全删除时间。

[0049] 如前所述，只有将数据从存储介质上擦除才能保证无法从存储介质上将所述数据恢复出来。但是，在SSD中，被删除的数据所在的存储介质页被标记为无效，而并没有从存储介质上擦除。根据本发明实施例，为敏感数据设置安全删除时间，从而指示该敏感数据在删除后的多长时间内应该被从存储介质上擦除。可以理解，越敏感的数据，其安全删除时间越短。对于敏感等级最高的数据，可以将安全删除时间设置为0，从而保证该敏感数据在被删除后立即被擦除。

[0050] 由于只有在垃圾回收操作时该存储介质页上的数据才会被擦除，并且垃圾回收操作是以存储介质块为最小单位的，因此所述安全删除时间指的也是所述敏感数据被删除和对所述敏感数据所在的存储介质块进行垃圾回收操作之间的最大时间间隔。

[0051] 根据本发明的一个实施例，可以在写入所述敏感数据时设置其安全删除时间，然后将所述安全删除时间与该敏感数据相关联地存储在SSD中。根据本发明另一个实施例，所述安全删除时间也可以在删除所述敏感数据时设置。这样做的好处是不需要额外的SSD存储空间来存储与敏感数据对应的安全删除时间。例如，所述安全删除时间的值可以包含在所述数据删除指令中。作为替换地，也可以在所述数据删除指令之前或之后，用单独的指令来将所述安全删除时间的值从操作系统传递给SSD。

[0052] 步骤203，响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间，设置所述剩余时间的值为所述安全删除时间。

[0053] 在有的SSD中，周期性地进行垃圾回收操作，即垃圾回收操作是由定时触发的。在这种情况下，距离下次垃圾回收操作的剩余时间具有确定的值。相应地，可以直接比较所述剩余时间和所述安全删除时间。

[0054] 在有的SSD中，垃圾回收操作是由事件触发的，而不是由定时触发的。例如，可能在SSD的空闲存储空间不足的情况下触发垃圾回收操作，或者在SSD的I/O负载低于一定阈值的时候触发垃圾回收操作。在这种情况下，可以直接认为所述剩余时间大于所述安全删除时间，从而设置所述剩余时间的值为所述安全删除时间。这之后，所述剩余时间具有确定的值，从而在后续再次执行步骤202时，可以直接比较所述剩余时间和其他的安全删除时间。

[0055] 步骤204，根据所述剩余时间触发垃圾回收操作。

[0056] 可以理解，剩余时间逐渐变少。在剩余时间变为零时，触发对垃圾回收队列中的指示符所指示的目标块进行的垃圾回收操作。这些存储介质块中的有效存储介质页中的数据会被转移到其他的存储介质块，然后这些存储介质块被擦除。相应地，这些存储介质块中的敏感数据也被擦除。

[0057] 采用根据本发明实施例的方案，敏感数据被删除后，其所在的存储介质块被放入垃圾回收队列。在该敏感数据所对应的安全删除时间之内，SSD会执行至少一次垃圾回收操作，从而该敏感数据所在的存储介质块会被擦除。这样就保证了在删除敏感数据后的一定时间内擦除敏感数据。对于某些敏感数据，可以将所述安全删除时间设置为0。这样在删除所述敏感数据后，紧接着就会触发垃圾回收操作，从而将所述敏感数据擦除。

[0058] 下面参照图3描述根据本发明实施例如何实现将敏感数据和非敏感数据存储在不同的存储介质块中。

[0059] 步骤301，接收数据写入指令，所述数据写入指令包括数据，并且所述数据写入指令指示所述数据是否为敏感数据。

[0060] 在根据本发明实施例的方案中，需要对操作系统进行一定的增强，使得操作系统发给SSD的数据写入指令可以指示该数据是否为敏感数据。可以在向操作系统安装SSD的驱动程序时进行所述增强，也可以通过在操作系统中打补丁来进行所述增强。

[0061] 根据本发明实施例，所述数据写入指令可以包括一个标记(flag)。SSD可以根据所述标记的值来判断所述数据是否为敏感数据。根据本发明另一个实施例，可以设置两条不同的数据写入指令。SSD可以根据收到的是哪条数据写入指令来判断所述数据是否为敏感数据。

[0062] 来自操作系统的数据写入指令除了包括数据本身以外，还包括对应于该数据的逻辑地址。可以事先在SSD和操作系统之间约定，操作系统在存储敏感数据时，只会使用某一

特定范围的逻辑地址。这样，SSD可以根据数据写入指令中所包含的逻辑地址来判断所述数据是否为敏感数据。这样做的好处是不用对所述数据写入指令的格式进行任何修正。

[0063] 步骤302，响应于所述数据是敏感数据，将所述数据存储在专用于存储敏感数据的存储介质块中。

[0064] 如果所述数据是敏感数据，那么从专用于存储敏感数据的存储介质块中分配一个存储介质页，并且将这个存储介质页的物理地址与所述逻辑地址关联。

[0065] 一般来说，如果一个存储介质块中包括空闲的存储介质页，那么SSD会一直在这个存储介质块中分配空间，直到这个存储介质块中不存在空闲的存储介质页；这之后，SSD会在一个新的存储介质块中分配存储空间。

[0066] 具体到本发明实施例的场合，SSD会记录当前正在被用来存储敏感数据的存储介质块，将这样的存储介质块称为当前敏感存储介质块。如果当前敏感存储介质块中包括空闲的存储介质页，那么SSD在当前敏感存储介质块中分配存储介质页来存储数据写入指令中的数据。如果当前敏感存储介质块中不包括空闲的存储介质页，那么SSD将一个新的存储介质块标注为当前敏感存储介质块，然后从这个新的存储介质块中分配存储介质页。可以理解，这个新的存储介质块需要满足的条件是，该存储介质块中不包含有效(valid)的用于存储非敏感数据的存储介质页。

[0067] 步骤303，设置所述敏感数据的安全删除时间，所述安全删除时间指示所述敏感数据被删除和被擦除之间的最大时间间隔。

[0068] 如前所述，除了在删除敏感数据时设置对应的安全删除时间以外，还可以在将敏感数据存储到SSD的时候就设置其安全删除时间。为了达到这一目的，安全删除时间的值可以包含在来自操作系统的所述数据写入指令中。SSD在收到所述数据写入指令后，根据其中包含的安全删除时间的值，设置该敏感数据的安全删除时间。作为替换地，也可以在所述数据写入指令之前或之后，用单独的指令来将所述安全删除时间的值从操作系统传递给SSD。

[0069] 采取如上所述的方法，敏感数据和非敏感数据被隔离地存储在不同的存储介质块中。对于存储非敏感数据的存储介质块，由于不存在安全删除的问题，因此可以按照通常的做法对其进行垃圾回收操作。这种垃圾回收操作通常考虑到SSD的写入/擦除次数，从而对SSD的寿命影响不大。对于存储敏感数据的存储介质块，由于设置了安全删除时间，从而可以保证在所设置的时间内对所述敏感数据所在存储介质块进行垃圾回收操作，从而可以将所述敏感数据从存储介质上被擦除。这种垃圾回收操作虽然会对所涉及的存储介质块的使用寿命产生不利影响，但是这种影响仅限于用于存储敏感数据的存储介质块。显然，相对于向整个SSD写入大量伪数据的做法，如图2所示的方法延长了SSD的寿命。

[0070] 从前面的描述可以看出，根据本发明实施例，对于敏感数据和非敏感数据的处理有许多不同之处。例如，在将敏感数据写入到存储介质时，敏感数据可能要写入到专用于敏感数据的存储介质块，并且可能需要处理相对应的安全删除时间；敏感数据被删除后，需要立即将其所在的存储介质块放入垃圾回收队列，并且需要比较距离下次垃圾回收操作的剩余时间和与敏感数据对应的安全删除时间。

[0071] 因此，根据本发明实施例，采用两个不同的模块来分别处理敏感数据和非敏感数据。这两个模块既可以是两个硬件模块，也可以是两个软件模块。在软件实现的场合，可以将本发明实施例实施为FTL(File Translation Layer)。根据本发明实施例，SSD中包括两

个FTL，其中一个用于处理非敏感数据，另一个用于处理敏感数据。前者称为非敏感FTL，后者称为敏感FTL。对于非敏感FTL而言，其可以采用与现有FTL一样的方案。对于敏感FTL而言，其需要实现根据本发明实施例的针对敏感数据的一系列处理。相对于采用一个FTL来处理敏感数据和非敏感数据而言，采用两个FTL来分别处理敏感数据和非敏感数据的好处是，不需要在每次处理数据时都对该数据是否为敏感数据进行判断。无论以什么方式SSD得知某数据为敏感数据，那么SSD只需要将该数据交给敏感FTL即可。敏感FTL按照处理敏感数据的方式来处理对该数据的任何后续操作，而无需每次操作该数据时都先判断一遍该数据是否为敏感数据。

[0072] 根据本发明实施例的设备典型地可以通过运行于图1所示的示例性计算机系统上的计算机程序来实现。虽然图1所示的是通用的计算机系统的硬件结构，但是由于该计算机系统运行了所述计算机程序，实现了根据本发明实施例的方案，从而使得该计算机系统/服务器从通用计算机系统/服务器转变成根据本发明实施例的设备。

[0073] 此外，虽然根据本发明实施例的设备从整体上看是由同一通用计算机系统来实现的，但是组成该设备的各个装置或模块在本质上是由分立的硬件实现的。这是因为，所述通用计算机在运行所述计算机程序时，往往采用诸如分时或分处理器核的共享方式来实现各个装置或模块。以分时实现为例，在特定的时刻，该通用计算机系统作为专用于实现特定装置或模块的硬件；在不同时刻，该通用计算机系统作为专用于实现不同的装置或模块的不同硬件。因此，根据本发明实施例的设备是一系列由硬件方式实现的装置或模块的组合，从而并非仅仅是功能模块构架。相反，根据本发明实施例的设备也可以被理解为主要通过硬件方式实现根据本发明实施例解决方案的实体设备。

[0074] 图4示出了根据本发明实施例的进行存储控制的装置，该装置包括：

[0075] 存储介质块处理模块，配置为响应于收到针对敏感数据的数据删除指令，将敏感数据所在的存储介质页标记为无效，并且将所述敏感数据所在的存储介质块放入垃圾回收队列，其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位；

[0076] 安全删除时间确定模块，配置为确定与所述敏感数据对应的安全删除时间；

[0077] 剩余时间设置模块，配置为响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间，设置所述剩余时间的值为所述安全删除时间；和

[0078] 触发模块，配置为根据所述剩余时间触发垃圾回收操作。

[0079] 所述装置进一步包括：

[0080] 写入指令接收模块，配置为接收数据写入指令，所述数据写入指令包括数据，并且所述数据写入指令指示所述数据是否为敏感数据；和

[0081] 数据存储模块，配置为响应于所述数据是敏感数据，将所述数据存储在专用于存储敏感数据的存储介质块中，

[0082] 其中，所述专用于存储敏感数据的存储介质块不包括有效的用于存储非敏感数据的存储介质页。

[0083] 其中所述安全删除时间在删除所述敏感数据时设置。

[0084] 其中所述安全删除时间在写入所述敏感数据时设置。

[0085] 其中采用不同的模块分别处理敏感数据和非敏感数据。

[0086] 附图中的流程图和框图显示了根据本发明的多个实施例的系统、方法和计算机程

序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，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，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0087] 以上已经描述了本发明的各实施例，上述说明是示例性的，并非穷尽性的，并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择，旨在最好地解释各实施例的原理、实际应用或对市场中的技术的技术改进，或者使本技术领域的其它普通技术人员能理解本文披露的各实施例。

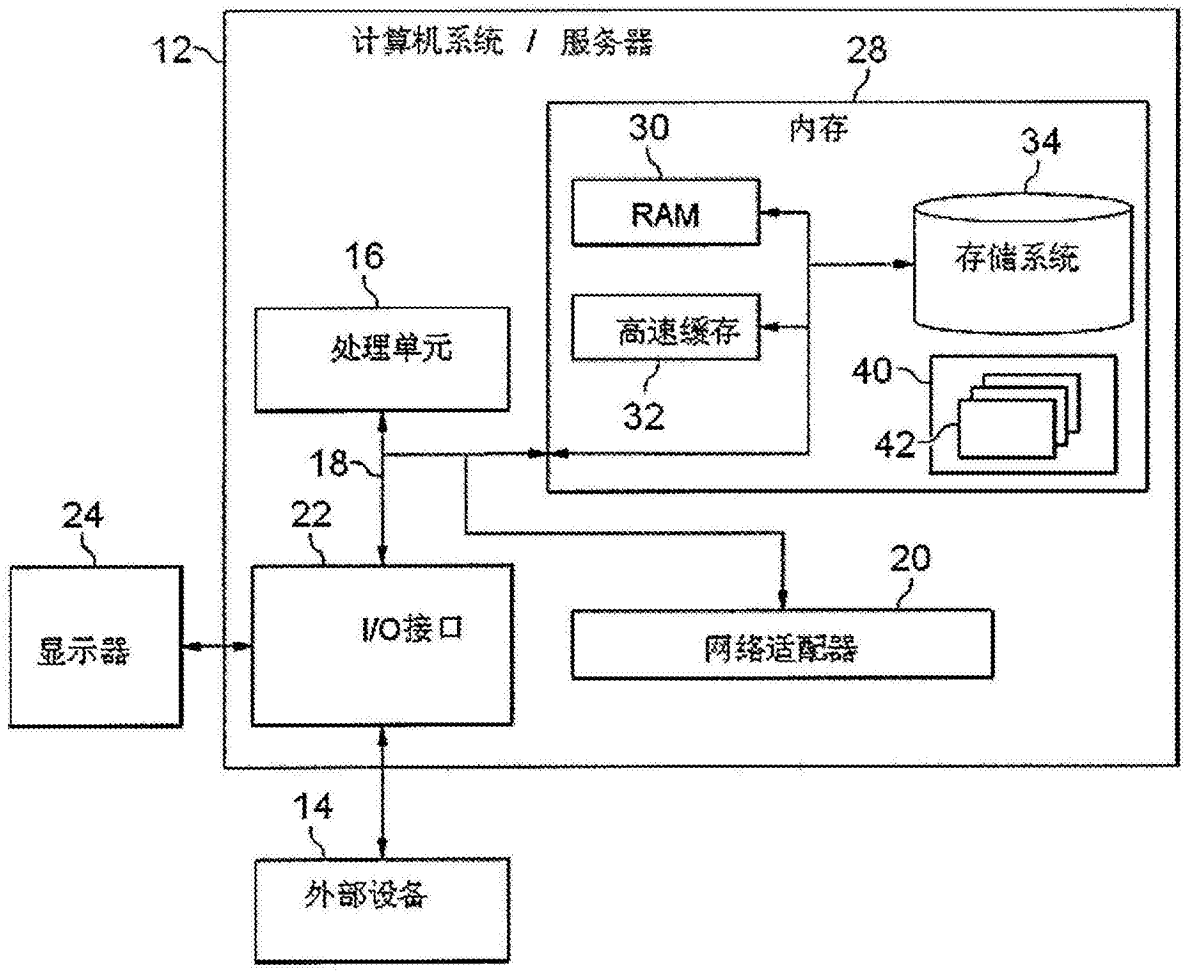

12
计算机系统 / 服务器
28
30
内存
34
RAM
存储系统
16
处理单元
高速缓存
32
40
42
18
24
22
20
显示器
I/O接口
网络适配器
14
外部设备

图1

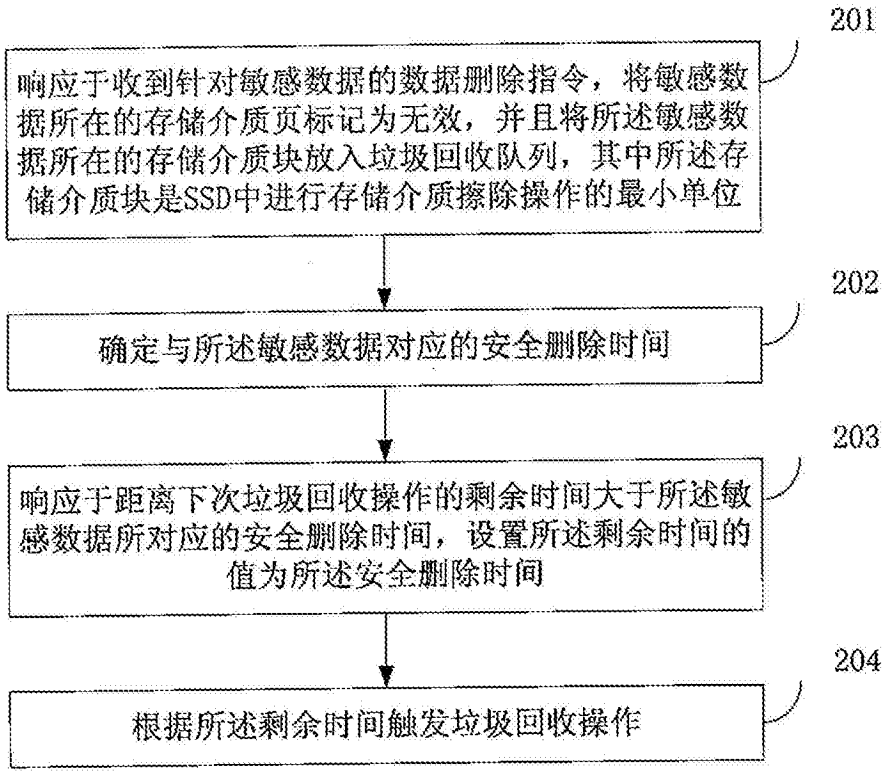

201
响应于收到针对敏感数据的数据删除指令，将敏感数据所在的存储介质页标记为无效，并且将所述敏感数据所在的存储介质块放入垃圾回收队列，其中所述存储介质块是SSD中进行存储介质擦除操作的最小单位
202
确定与所述敏感数据对应的安全删除时间
203
响应于距离下次垃圾回收操作的剩余时间大于所述敏感数据所对应的安全删除时间，设置所述剩余时间的值为所述安全删除时间
204
根据所述剩余时间触发垃圾回收操作

图2

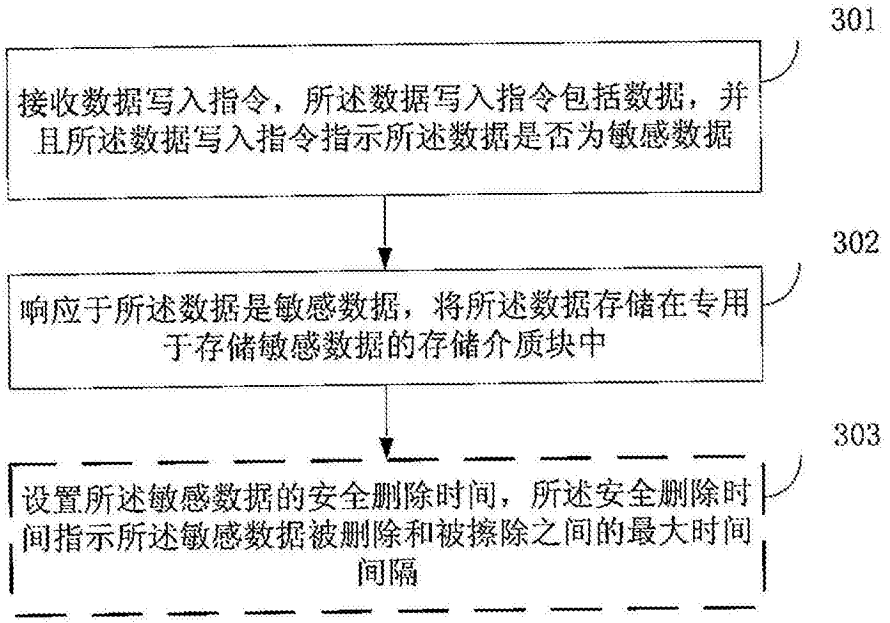

301
接收数据写入指令，所述数据写入指令包括数据，并且所述数据写入指令指示所述数据是否为敏感数据
302
响应于所述数据是敏感数据，将所述数据存储在专用于存储敏感数据的存储介质块中
303
设置所述敏感数据的安全删除时间，所述安全删除时间指示所述敏感数据被删除和被擦除之间的最大时间间隔

图3

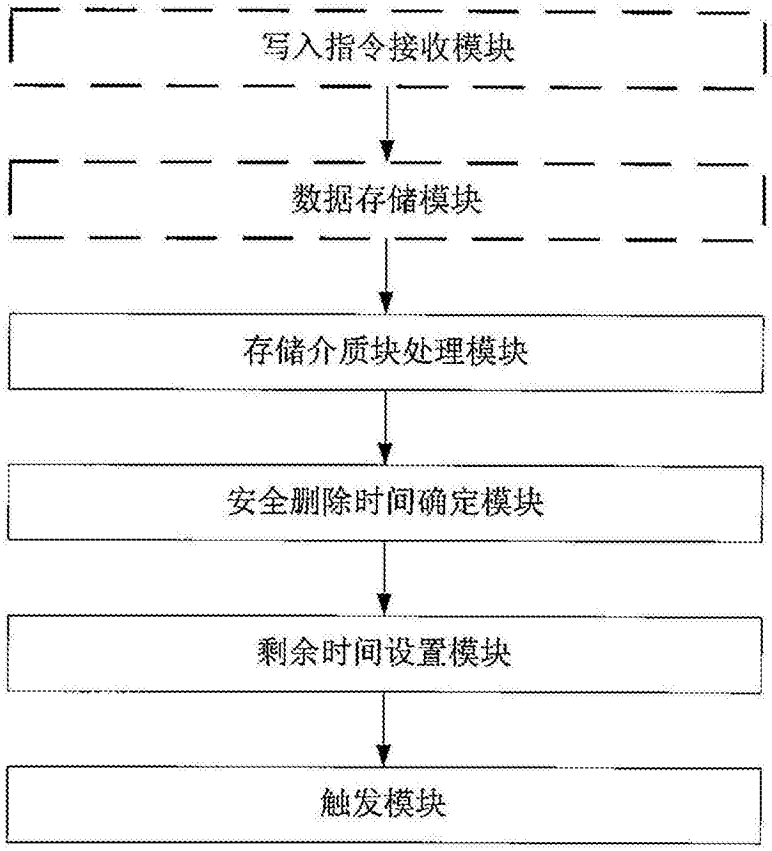


图4