[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06F 9/445 (2006.01)

[12] 发明专利说明书

专利号 ZL 200580014377.1

[45] 授权公告日 2009 年 5 月 27 日

[11] 授权公告号 CN 100492324C

[22] 申请日 2005.3.4
[21] 申请号 200580014377.1
[30] 优先权
[32] 2004.3.5 [33] AU [31] 2004901143
[86] 国际申请 PCT/AU2005/000317 2005.3.4
[87] 国际公布 WO2005/086005 英 2005.9.15
[85] 进入国家阶段日期 2006.11.6
[73] 专利权人 安全系统有限公司
地址 澳大利亚西澳大利亚
[72] 发明人 迈克尔·J·温
迈克尔·R·格迪斯
[56] 参考文献
WO03/100544A2 2003.12.4
US6463537B1 2002.10.8
Pointsec PC 4.3 Security Target, ST Version 1.08. Pointsec Mobile Technologies, Inc. Pointsec PC 4.3 Security Target, ST Version 1.08. 2004
审查员 曾威
[74] 专利代理机构 北京市柳沈律师事务所
代理人 蒲迈文 黄小临

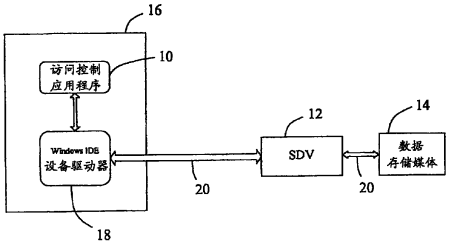
权利要求书 3 页 说明书 13 页 附图 11 页

[54] 发明名称

控制分区访问的分区访问控制系统和方法

[57] 摘要

本发明公开了一种控制对存储在计算机系统的至少一个数据存储媒体(14)上的数据的访问的访问控制系统(10)。该访问控制系统(10)包含验证装置(25)，用于验证允许访问存储在至少一个数据存储媒体(14)中的数据的用户；和数据库装置(29)，被安排成存储数据访问简要表。每个数据访问简要表与允许访问存储在至少一个数据存储媒体(14)中的数据的用户相联系，每个数据访问简要表包括指示允许用户访问存储在至少一个数据存储媒体(14)中的数据的访问度的信息，和每个数据访问简要表包括主数据访问简要表(M)和当前数据访问简要表(C)。当前数据访问简要表(C)可在主数据访问简要表(M)定义的参数内修改。



1. 一种控制对存储在计算系统的至少一个数据存储媒体上的数据的访问的访问控制系统，该访问控制系统包含:

验证装置，用于验证允许访问存储在至少一个数据存储媒体中的数据的用户；和

数据库装置，被安排成存储数据访问简要表;

每个数据访问简要表与允许访问存储在至少一个数据存储媒体中的数据的用户相联系;

每个数据访问简要表包括指示允许用户访问存储在至少一个数据存储媒体中的数据的访问度的信息；和

每个数据访问简要表包括主数据访问简要表和当前数据访问简要表，当前数据访问简要表可在主数据访问简要表定义的参数内修改。

2. 根据权利要求 1 所述的访问控制系统，进一步包含被安排成促进创建主数据访问简要表和当前数据访问简要表的简要表设置装置。

3. 根据权利要求 2 所述的访问控制系统，其中，将访问控制系统合并到含有操作系统的计算系统中，和主数据访问简要表只可以在装载操作系统之前修改。

4. 根据权利要求 1 到 3 的任何一项所述的访问控制系统，其中，所述访问控制系统是可激活的，以便允许修改当前数据访问简要表，并且所述访问控制系统是可去激的，以便防止修改当前数据访问简要表。

5. 根据权利要求 1 所述的访问控制系统，其中，访问控制系统至少部分以软件的形式实现。

6. 根据权利要求 1 所述的访问控制系统，其中，访问控制系统至少部分以硬件的形式实现。

7. 根据权利要求 1 所述的访问控制系统，其中，访问控制系统被安排成支配配置成控制对数据存储媒体的访问的保密设备使用的用户访问简要表。

8. 根据权利要求 7 所述的访问控制系统，其中，保密设备至少部分用硬件实现，和是位于计算系统的存储媒体与计算系统的 CPU 之间的那种类型。

9. 根据权利要求 7 所述的访问控制系统，其中，保密设备至少部分用硬件实现，并且是合并到计算系统的总线桥接电路中的那种类型。

10. 根据权利要求 1 所述的访问控制系统，其中，将访问控制系统合并到含有操作系统的计算系统中，并且当前数据访问简要表可以在装载操作系统之后修改。

11. 一种使用访问控制系统来控制对存储在计算系统的至少一个数据存储媒体上的数据的访问的方法，该方法包含如下步骤:

提供验证允许访问存储在至少一个数据存储媒体中的数据的用户的装置;

存储数据访问简要表;

将每个数据访问简要表与允许访问存储在至少一个数据存储媒体中的数据的用户相联系;

每个数据访问简要表包括指示允许用户访问存储在至少一个数据存储媒体中的数据的访问度的信息; 和

每个数据访问简要表包括主数据访问简要表和当前数据访问简要表; 和

促进在主数据访问简要表定义的参数内修改当前数据访问简要表。

12. 根据权利要求 11 所述的方法，其中，进一步包含促进创建主数据访问简要表和当前数据访问简要表的步骤。

13. 根据权利要求 12 所述的方法，其中，将访问控制系统合并到含有操作系统的计算系统中，和促进修改当前数据访问简要表的步骤包括只在装载操作系统之前促进修改主数据访问简要表的步骤。

14. 根据权利要求 11 到 13 的任何一项所述的方法，进一步包括促进激活所述访问控制系统，以便允许修改当前数据访问简要表，和促进去激所述访问控制系统，以便防止修改当前数据访问简要表的步骤。

15. 根据权利要求 11 所述的方法，其中，访问控制系统至少部分以软件的形式实现。

16. 根据权利要求 11 所述的方法，其中，访问控制系统至少部分以硬件的形式实现。

17. 根据权利要求 11 所述的方法，进一步包括将访问控制系统安排成支配配置成控制对数据存储媒体的访问的保密设备使用的用户访问简要表的步骤。

18. 根据权利要求 17 所述的方法，其中，保密设备至少部分用硬件实现，并且是位于计算系统的存储媒体与计算系统的 CPU 之间的那种类型。

19. 根据权利要求 17 所述的方法，其中，保密设备至少部分用硬件实现，并且是合并到计算系统的总线桥接电路中的那种类型。

20. 根据权利要求 11 所述的方法，进一步包括将访问控制系统合并到含有操作系统的计算系统中，和在装载操作系统之后促进修改当前数据访问简要表的步骤。

控制分区访问的分区访问控制系统和方法

技术领域

本发明涉及特别用于控制用户访问计算系统的数据存储媒体的计算机的分区访问控制系统和方法。

在整个说明书中，除非上下文另有要求，词语“包含”或像“包括”或“含有”那样的变体应该理解为内含陈述的整数或整数组，但不排除任何其它整数或整数组。

背景技术

下面对背景技术的讨论只是为了便于人们了解本发明。应该体会到，这个讨论不是确认或承认涉及的任何内容都是直到本申请的优先权日人所共知的知识部分。

随着计算机联网技术和计算机一般性使用的广泛发展，为了防止用户和像病毒、蠕虫和其它类型的恶性软件那样的程序的非授权访问，计算机系统，尤其通过这样的系统访问存储媒体上的数据的保密性问题已经变得极为重要。

提供通过为每个用户定义对存储在存储媒体上的数据的访问许可，和要求在授权访问存储媒体之前利用，例如，用户名和通行字验证用户，提供对未授权访问的预防度的操作系统是众所周知的。

但是，这样的安排只提供对未授权访问数据存储媒体的最小预防度。

在牵涉到插在主机中央处理单元（CPU）和计算机的海量数据存储媒体之间的分立保密设备的使用的计算机系统中提供保证数据和信息存储的系统和方法是众所周知的。

提供整合到配备在计算机系统的母板上的总线桥接电路中或整合到配备在硬盘驱动器本身中的总线桥接电路中的保密设备也是众所周知的。

对于这两种安排，在系统管理器控制下的保密设备能够为配备在计算机系统的海量存储媒体上分区和为计算机系统的每个用户设置数据访问许可。数据访问许可包括只读访问、只写访问、读写访问、或无法访问。在本说明

书中，将为特定用户定义的一组数据访问许可命名为“用户访问简要表”。

为了保证合并了保密设备的计算机系统的完整性，保密设备被配置成只验证用户，和在装载计算机操作系统之前，在启动计算机系统时将用户访问简要表指定给用户。在装载了操作系统之后不可能再对特定用户的用户访问简要表进行修改。

但是，虽然这样的安排提供了高度保密性，但在针对各种环境，例如，当与因特网连接或不与因特网连接时，将多个用户访问简要表指定给用户的情况下，相对来说这种安排给用户带来不便。在这种情况下，如果按照不允许因特网访问的访问简要表登录用户，那么，为了访问因特网，要求用户关掉操作系统，和在启动过程的验证阶段采用适合与因特网连接的不同用户简要表。

这样的过程给系统的用户带来不便，并且，可以明显地降低工作效率。

发明内容

按照本发明的第一方面，提供了控制对存储在计算机系统的至少一个数据存储媒体上的数据的访问的访问控制系统，该访问控制系统包含:

验证装置，用于验证允许访问存储在至少一个数据存储媒体中的数据的用户；和

数据库装置，被安排成存储数据访问简要表;

每个数据访问简要表与允许访问存储在至少一个数据存储媒体中的数据的用户相联系;

每个数据访问简要表包括指示允许用户访问存储在至少一个数据存储媒体中的数据的访问度的信息；和

每个数据访问简要表包括主数据访问简要表和当前数据访问简要表，当前数据访问简要表可在主数据访问简要表定义的参数内修改。

在一种安排中，访问控制系统进一步包含被安排成促进创建主数据访问简要表和当前数据访问简要表的简要表设置装置。

可以将访问控制系统合并到含有操作系统的计算系统中，和主数据访问简要表只可以在装载操作系统之前修改。

在一个实施例中，控制系统是可激活的，以便允许修改当前数据访问简要表，和可去激的，以便防止修改当前数据访问简要表。

访问控制系统至少部分可以以软件的形式实现。

另外，或可替代地，访问控制系统至少部分可以以硬件的形式实现。

在一个实施例中，访问控制系统被安排成支配配置成控制对数据存储媒体的访问的保密设备使用的用户访问简要表。保密设备至少部分可以用硬件实现，和可以是位于计算机系统的存储媒体与计算系统的 CPU 之间的那种类型。可替代地，保密设备至少部分可以用硬件实现，和可以是合并到计算系统的总线桥接电路中的那种类型。

在一种安排中，将访问控制系统合并到含有操作系统的计算系统中，和当前数据访问简要表可以在装载操作系统之后修改。

按照本发明的第二方面，提供了控制对存储在计算系统的至少一个数据存储媒体上的数据的访问的方法，该方法包含如下步骤:

提供验证允许访问存储在至少一个数据存储媒体中的数据的用户的装置;

存储数据访问简要表;

将每个数据访问简要表与允许访问存储在至少一个数据存储媒体中的数据的用户相联系;

每个数据访问简要表包括指示允许用户访问存储在至少一个数据存储媒体中的数据的访问度的信息; 和

每个数据访问简要表包括主数据访问简要表和当前数据访问简要表; 和

促进在主数据访问简要表定义的参数内修改当前数据访问简要表。

按照本发明的第三方面，提供了当装入计算系统中时，使计算系统按照访问控制系统操作的计算机程序，该访问控制系统用于控制对存储在计算系统的至少一个数据存储媒体上的数据的访问，该访问控制系统包含:

验证装置，用于验证允许访问存储在至少一个数据存储媒体中的数据的用户; 和

数据库装置，被安排成存储数据访问简要表;

每个数据访问简要表与允许访问存储在至少一个数据存储媒体中的数据的用户相联系;

每个数据访问简要表包括指示允许用户访问存储在至少一个数据存储媒体中的数据的访问度的信息; 和

每个数据访问简要表包括主数据访问简要表和当前数据访问简要表，当

前数据访问简要表可在主数据访问简要表定义的参数内修改。

按照本发明的第四方面，提供了含有使计算机按照访问控制系统操作的计算机可读程序代码的计算机可用媒体，该访问控制系统用于控制对存储在计算系统的至少一个数据存储媒体上的数据的访问，该访问控制系统包含:

验证装置，用于验证允许访问存储在至少一个数据存储媒体中的数据的用户；和

数据库装置，被安排成存储数据访问简要表;

每个数据访问简要表与允许访问存储在至少一个数据存储媒体中的数据的用户相联系;

每个数据访问简要表包括指示允许用户访问存储在至少一个数据存储媒体中的数据的访问度的信息；和

每个数据访问简要表包括主数据访问简要表和当前数据访问简要表，当前数据访问简要表可在主数据访问简要表定义的参数内修改。

附图说明

现在参照附图对本发明进行描述，在附图中:

图 1 是示出包括按照本发明第一实施例的分区访问控制系统的计算系统的方块图，所示的访问控制系统与安排成保护计算机系统数据存储媒体那种类型的保密设备（SDV）相联系;

图 2 是如图 1 所示的访问控制系统和与访问控制系统交接的 SDV 的逻辑结构的方块图;

图 3 描绘了通过如图 1 和 2 所示的访问控制系统的图形用户界面（GUI）显示的主屏幕，主屏幕示出了配备在计算机系统的数据存储媒体上的分区和可用于计算机系统的特定用户的数据访问许可;

图 4 是示出合并了如图 1 和 2 所示的访问控制系统和 SDV 的计算机系统的初始化过程的流程图;

图 5 是 GUI 为“超级用户”访问包括图 1 和 2 所示的访问控制系统的计算机系统和初始化用户访问简要表而显示的面板;

图 6 是为了验证“超级用户”的目的而显示的面板;

图 7 是为了配置用户访问简要表的目的而向“超级用户”显示的面板;

图 8 是为了在配置用户简要表期间为特定分区定义数据访问许可的目的

而叠加在图 7 的显示面板上的面板;

图 9 是示出调用访问控制系统时用户执行的逻辑进程的流程图;

图 10 示出了验证访问访问控制系统的用户的通行字输入框;

图 11 示出了被验证使用访问控制系统的用户的分区访问控制表;

图 12 是示出合并了 SDV 和访问控制系统进程流的计算机系统的正常系统操作的流程图; 和

图 13 示出了在引导操作系统之前在向 SDV 验证用户期间向典型用户显示的用户验证框。

本发明实施例描述

现在参照附图, 图中所示的是在本例中以应用软件的形式实现和被配置成与被安排成控制和协调对计算系统的海量数据存储媒体的访问的保密设备相联系进行操作的分区访问控制系统。

但是, 虽然本实施例是结合以软件形式实现的访问控制系统进行描述的, 但应该明白, 其它安排也是可以的。例如, 访问控制系统至少部分可以用硬件实现。

还应该明白, 保密设备的存在不是本发明必需的, 其它安排也是可以的。例如, 根据本发明的访问控制系统可以被配置成与操作系统的适当访问控制应用程序相联系进行操作。

上述实施例针对被安排成控制用户访问数据存储媒体, 和允许用户在预定参数内修改相应用户数据访问简要表的访问控制系统。

在本实施例中, 合并了访问控制系统的计算机系统具有标准个人计算机 (PC) 的形式, 标准个人计算机包含中央处理单元 (CPU)、像监视器、键盘、鼠标和打印机那样的标准外围设备、像硬盘驱动器 (HDD) 那样具有海量数据存储媒体形式的数据存储器、和用于控制和协调对海量数据存储媒体的数据访问的、描述在专利说明书 WO 03/003242 中那种类型的保密设备 (SDV)。

正如在专利说明书 WO 03/003242 中描述的那样, SDV 被插在 CPU 和 HDD 之间的数据访问通道中, 和控制用户对 HDD 的数据访问。这种控制是利用验证进程实现的, 从而许可访问 HDD 上的数据的用户在引导 PC 操作系统之前必须得到验证, 和必须配有与数据存储媒体的各种分区有关的确定用户的数据访问许可的特定分区访问简要表。并且, SDV 被设计成强迫系统验证的每个

特定用户执行数据访问体系，按照分区访问简要表拒绝对数据存储媒体一些部分的访问，和拒绝未得到验证的用户和/或通过假进程的访问。

正如所述的那样，在进行了“驱动器 ID”检验之后，在基本输入输出系统（BIOS）的操作期间调用验证进程，和取代通常存储在数据存储媒体中的正常引起扇区或主引导记录，一旦装载了 SDV 提供的“定制”引导扇区，就由 CPU 运行验证程序。

正如所述的那样，只有在已经适当地验证了用户和已经完成了在验证应用程序的操作期间用户承担的进程之后，BIOS 程序才继续允许访问数据存储媒体和装载用户随后可以按照相关数据访问简要表操作计算机和访问数据存储媒体的操作系统。

如图 1 所示，按照本实施例的分区访问控制系统被具体配置成与上述那种类型的保密设备（SDV）12 交互。在本例中，访问控制系统用软件实现成分区访问控制应用程序 10 和被存储在 PC 的数据存储媒体 14 中的某个位置中。

在本实施例中，访问控制应用程序 10 被写成用 VC++和 MFC 开发的 Windows 程序，以便在 Windows 操作系统 16 内运行，但是，应该明白，其它安排也是可以的。访问控制应用程序 10 通过 Windows 应用程序接口（API）与 Windows IDE 设备驱动器 18 交接，和沿着 IDE 电缆 20 与数据存储媒体 14 通信。如图所示，用导线将 SDV 12 与 IDE 电缆 20 连接起来，以便截取 Windows IDE 设备驱动器 18 与数据存储媒体 14 之间的所有通信。

为了与 SDV 12 和用户通信，访问控制应用程序 10 使用主机操作系统的 Windows API 提供的服务，主机操作系统可以是 Windows 2000 或 Windows XP。

但是，应该体会到，也可以将访问控制应用程序 10 安排成与像 LINUX 那样的其它操作系统交接。

如附图的图 2 所示，访问控制应用程序 10 包含具有验证器 25 和控制系统引擎 27 形式的逻辑进程，控制系统引擎 27 与可以形成 SDV 12 的一部分或可以形成数据存储媒体 14 的一部分的数据库 29 通信。

通常在操作系统 16 的控制下在 PC 的 CPU 21 的操作下调用访问控制应用程序 10 进行操作，并且，访问控制应用程序 10 与 SVD 引擎 35 交互，SVD 引擎 35 控制 CPU 31 与数据存储媒体 14 之间的数据访问。

如前所述，数据存储媒体 14 可以包含一个或多个 HDD，每个 HDD 含有一

个或多个分区。在本实施例中，驱动器/分区是C:\、D:\、E:\、F:\、G:\、H:\、和I:\。

访问控制应用程序10的控制系统引擎27包含被安排成以规定方式安置数据库29的简要表设置器37和编辑器39。这些部件将在后面作更详细描述。

数据库29被设计成为允许访问PC的数据存储媒体14的每个用户逻辑存储两种类型的数据访问简要表。数据访问简要表包括用户1到n的主数据访问简要表M1到Mn、和当前数据访问简要表C1到Cn。每个数据访问简要表为允许用户访问的那些分区定义特定用户的数据访问许可。

例如，如图3所示，图中示出了与用户简要表相联系的用户访问驱动器C:\、E:\、F:\、G:\、H:\、和I:\所指的六个分区42的用户简要表屏幕40，以及为每个分区指出了相应分区大小44。还示出了指示分区是否可引导、允许还是禁止分区访问控制、和应用于特定分区或驱动器的当前许可的进一步细节46。如在“当前许可”列中所指的那样，每个分区可用几种数据访问许可，即，“只读”、“只写”、“读/写”和“无法访问”。

访问控制应用程序10的验证器25独立地起SDV 12的验证程序的作用和被配备成验证允许使用访问控制应用程序10的用户。正如后面更详细描述的那样，SDV 12是这样配置的，允许SDV 12的管理者或“超级用户”配置允许访问PC的数据存储媒体14的用户的数据访问简要表。

验证器25与控制系统引擎27一道工作和通过SDV引擎35与数据库29交互，以便允许超级用户或正常用户利用对于用户的状态可应用的相应功能和相关主数据访问简要表访问访问控制应用程序10。

存储在数据库29内的每个数据访问简要表包括如下信息:

>每个允许用户的用户名和通行字;

>允许用户访问的数据存储媒体的分区；和

>允许用户访问的每个分区的许可状态。

每种许可状态用于定义对存储在每个分区内的数据的不同数据访问度，包括允许程度低或不允许、允许从分区中读取数据、允许将数据写入分区中、或从分区中读取数据或将数据写入分区中都允许。

在本实施例中，可能许可的范围如下:

无法访问－不允许读写数据;

只读－不允许写但允许读;

读/写－读写数据都允许。

简要表设置 37 被具体设计成允许设置主数据访问简要表和当前数据访问简要表。主数据访问简要表有效地设置用户可以利用访问控制应用程序 10 改变或变更用户的当前数据访问简要表的范围。

编辑器 39 可以被访问控制应用程序 10 的超级用户或正常用户调用，以便分别编辑主数据访问简要表或用户的当前数据访问简要表。因此，如果验证器 25 识别出超级用户，控制系统引擎 27 允许超级用户以访问和改变存储在数据库 29 内的 PC 的任何允许用户的主数据访问简要表的方式操作编辑器 39。如果验证器 25 将用户验证成正常允许用户，控制系统引擎 27 允许用户以允许在事先为用户确定的主数据访问简要表定义的参数内修改验证用户的当前数据访问简要表的方式操作编辑器。

因此，应该明白，主数据访问简要表定义的参数只允许将分区的数据访问许可修改成相同或较低的数据访问度。重要的是，主数据访问简要表定义的参数不允许将特定分区的数据访问许可修改成比在主数据访问简要表中为允许用户规定的数据访问度高的数据访问度。

举例来说，如果与用户相联系的主数据访问简要表规定用户对分区或驱动器 E:\进行“只读”访问，那么，用户只能将驱动器 E:\的当前数据访问许可修改成“无法访问”。不能将驱动器 E:\的数据访问许可修改成“读/写”访问。

同理，如果与用户相联系的主数据访问简要表规定用户对驱动器或分区 E:\“无法访问”，那么，拒绝用户对驱动器或分区 E:\的当前数据访问许可作任何改变。

因此，简要表设置器 37 只允许当前数据访问简要表经过 SDV 引擎 35，供以后与用户的主数据访问简要表的参数相符的 SDV 12 使用。

为了更好地了解如何为进程流和通过作为 Windows API 的一部分配备的图形用户界面（GUI）与用户的交互配置访问控制应用程序 10，现在结合图 4 到 13 描述访问控制应用程序的操作。

在图 4 中示出了初始化阶段 SDV 12 执行的软件流程。

通过用导线将 SDV 硬件 12 与 IDE 电缆 20 连接起来将 SVD 硬件 12 安装在 CPU 31 与数据存储媒体 14 之间用 41 表示。然后在 43 中用所需多个分区格式化数据存储媒体 14 的 HDD，在 45 中在 PC 的操作系统的控制下安装 HDD。

在 47 中将包含 SDV 12 的设置软件的 CD ROM 插入 PC 的 CD ROM 驱动器中，和在操作系统 16 的控制下装载设置程序。

如果 SDV 12 还没有初始化，则在 49 中软件流程调用 51 中设置 SDV 12 的超级用户的进程。超级用户能够为 PC 的所有允许用户设置用户名和通行字和他们的相关主数据访问简要表。这个进程调用 53 中的 GUI，以创建如附图的图 5 所示的超级用户显示面板 55。显示面板 55 允许创建超级用户名和为超级用户设置通行字。显示面板 55 还允许超级用户在需要的时候允许与 PC 的允许用户有关的访问控制，和设置超级用户的访问控制通行字，以及访问控制通行字的确认、和身份字符串，以便调用访问控制应用程序 12 时验证超级用户。在屏幕的底部还配备了“完成”按钮 57，以便允许用户在 59 中退出进程。

一旦创建了超级用户帐户，就认为 SDV 12 已初始化和进入用户帐户配置状态，在用户帐户配置状态下，超级用户可以为允许访问 PC 的用户设置独立用户帐户，为对他们的验证创造条件。

如图所示，软件流程可以在通过退出进程 59 或者判定框 49 判定是否 SDV 12 以前已初始化而设置了超级用户之后马上在步骤 61 对超级用户配置用户帐户。通过显示如附图的图 6 所示的用户验证面板 63，和提示超级用户在 65 中输入他们用于正确验证的用户名和通行短语，该进程从 61 开始。在显示面板 63 上配备了验证按钮 67，以便在 69 中实现验证。如果超级用户在这个阶段未得到验证，则程序流从 71 退出，需要重新开始 SDV 12 的设置程序，和重复该过程，直到验证了超级用户的时候。

一旦在 69 中得到有效验证，软件就调用 73 中允许创建每个独立用户帐户的进程，指定独立用户通用短语和访问权，以便为独立用户配置主数据访问简要表。

这个进程使用了如图 7 所示的显示面板 75，以便在 77 中配置每个独立用户简要表。显示面板 75 包括用于输入用户名、通行字、通行字确认、访问控制通行字、访问控制通行字确认和身份字符串的数据输入字段。显示面板 75 还包括两个分区面板，第一分区面板 79 列出在数据存储媒体 14 的 HDD 上格式化的各自分区，和第二分区面板 81 列出超级用户选择的供特定用户访问用的分区。

如图 7 所示，为每个格式化和所选分区配备了分区名和存储器地址映像。

在显示面板 75 的底部配备了“保存”按钮 83 和“返回到主菜单”按钮 85，以便分别保存配置和返回到正常程序流。

为了为独立用户选择分区访问、许可和访问控制可达性，调用使 GUI 示出如图 8 所示的叠加在用户简要表配置面板 75 上的显示面板 89 的进程 87。

显示面板 89 允许识别与用户的特定分区访问有关的开始扇区地址、分区大小、访问模式和访问控制模式的设置。如图所示，为“访问模式”和“访问控制模式”输入字段分别配备了下落式菜单，以便允许为设置访问模式而选择固定许可访问模式，即，只读、读/写和无法访问，和为设置访问控制模式而选择“允许”或“禁止”。在显示面板 91 的底部配备了“OK”按钮 93 和“取消”按钮 95，以便为完成加亮分区的分区细节选择创造条件。

在完成了每个用户简要表配置之后，在 97 中对超级用户是否配置了所有用户进行检验，如果不是，为另一个用户执行用户简要表配置步骤 73。如果所有用户的简要表配置都已完成，如步骤 99 所示，则停止初始化过程。

如前所述，在本例中，访问控制应用程序 10 起操作系统 16 下面的应用程序的作用，和与 Windows API 交互，以便与用户和 SDV 引擎 35 通信。在图 9 中示出了访问控制应用程序 10 的软件流程。

用户在 101 中调用访问控制应用程序 10，和显示如图 10 所示的通行字输入显示面板 105。显示面板 105 用于输入验证用户的相关访问控制通行字。

显示面板 105 包括“登录”按钮 107 和“退出”按钮 109，以便继续或退出访问控制验证进程。如果按下“登录”按钮 107 继续下去，访问控制应用程序 10 就在 111 中与 SDV 12 通信以便进行验证，在 113 中据此核实验证。如果用户未得到验证，则用户在 103 中输入相关访问控制通行字。如果用户得到验证，该进程继续进行下去和控制系统引擎 27 在 115 中从 SDV 11 中检索分区访问控制信息。

然后，以如图 11 所示的表格 117 的形式向用户显示验证用户的分区访问控制信息。表格 117 对应于前面在附图的图 3 中所述的表格，和只显示超级用户分配给用户访问的那些分区。为用户配备了将在表格中规定的许可修改成简要表设置器 37 允许的程度的选项，也就是说，可以按照主访问简要表在“当前许可”列下降低或重申数据访问度。这是通过如下操作实现的，那就是，点击“当前许可”的特定项目，据此给出下落式菜单，下落式菜单提供可为特定驱动器选择的和在超级用户事先为用户设置的主数据访问简要表确

定的控制范围内的可用许可。

在显示面板 117 的底部配备了“应用”按钮 121 和“关闭”按钮 123，以便使软件流程在 125 中可以前进。此外，如果用户未修改任何分区访问控制和按下“关闭”按钮 123，那么，访问控制应用程序 10 直接从 127 退出。如果用户修改了当前许可和通过按下“应用”按钮 121 应用它们，那么，简要表设置器 37 在 129 中将分区访问控制信息发送到 SDV 12，以便适当地修改存储在数据库 29 中的相关当前数据访问简要表。

在图 12 中示出了访问控制应用程序的正常软件流程与正常 SDV 系统操作的整合。相同的步骤用相同的标号表示。

在 SDV 12 和访问控制应用程序 10 的正常操作期间，在 131 中对 PC 加电，和在 133 中随后调用它的计算机 BIOS 装载来自 SDV 引导设备的启动代码。

在 135 中提示用户在 139 中通过经由 GUI 向用户显示的用户验证显示面板 137 输入相关名称和通行短语。一旦按下配备在显示面板 137 底部的“验证”按钮 141，就调用 SDV 验证进程，以验证用户是否是计算机系统的允许用户。

如果用户在 143 中未得到验证，然后，将尝试计数加 1（或减 1）和在 145 中检验是否超过允许验证尝试次数。如果超过允许验证尝试次数，软件进程从 147 退出和关闭计算机系统。如果还没有达到验证用户的允许尝试数据，那么，软件流程返回，在 135 中提示用户输入相关名称和通行短语，以便向用户提供另一次验证尝试。

一旦用户在 143 中得到验证，SDV 12 就在 149 中解密在本实施例中存储在存储器的隐藏区中的数据库 29 中的有效用户分区访问信息，以便按照为允许用户配置的当前用户简要表控制对数据存储器的随后数据访问。

然后在 151 中启动计算机操作系统 16，由此，SDV 12 在 153 中按照允许用户的当前数据访问简要表检验对数据存储媒体 14 的所有随后数据访问。如果 155 中的数据访问尝试与用户的当前数据访问简要表不一致，那么，在 157 中阻止“读”或“写”的数据传送进程，不实现对 HDD 的任何访问。然后，SDV 12 返回到 153 中它的数据检验状态。

如果在 155 中数据访问与用户的当前数据访问简要表一致，那么，在 159 中检验数据，以查明是否正在调用访问控制应用程序。如果不是，在 161 中继续对数据存储器 15 的 HDD 的数据访问，和在 163 中检验断电条件。如果在

163 中肯定断电条件，软件流程从 165 退出和通过计算机系统实现断电进程。如果未肯定断电条件，那么，软件流程使 SDV 12 返回到 153 中它的数据检验状态。

如果在 159 中 SDV 12 确定已调用访问控制应用程序 10，那么，前进到参照图 9 所述的访问控制软件流程进程。

如果用户有效地访问访问控制应用程序 10，则访问控制应用程序 10 在 115 中读取存储在数据库 29 中的分区访问控制信息，和在 119 中显示用户的当前数据访问简要表。

如果用户在 125 中利用编辑器 39 修改相关访问权，那么，访问控制应用程序 10 在 129 中利用简要表设置器 37 更新存储在 SDV 的数据库 29 中的当前数据访问权，和访问控制应用程序 10 在 127 退出。另一方面，如果在 125 中未修改访问权，那么访问控制应用程序 10 直接从 127 退出。一旦使访问控制应用程序 10 退出，在 163 中再次检验断电条件，如果得到肯定，程序流从 165 退出。如果未得到肯定，那么，软件流程使 SDV 12 返回到 153 中它的数据检验状态。

在一个可替代实施例中，在计算机系统的 CPU 侧的母板的南桥中，或者，可替代地，正如在本申请人的国际申请 PCT/AU2004/000210 的国际专利说明书中描述的那样，在将串行 AT 嵌入式接口（SATA）标准用于与数据存储器的通信的情况下，在配备在数据存储器侧的桥接电路中，配备合并到总线桥接电路的设计中的 SDV 12。

应该体会到，在上面每个实施例中所述的控制系统都允许验证用户在操作系统下在正常系统操作期间改变用户已经得到授权的读/或写访问控制分区，而无需在引导前进程中改变用户简要表。因此，访问控制应用程序 10 作为标准应用软件安装在计算机系统的硬盘上和在操作系统的控制下运行。

这样，每个用户只需要一个主数据访问简要表，每个主数据访问简要表定义用户可访问的每个分区的数据访问许可和允许在主数据访问简要表的限定内访问分区。这意味着，可以完全控制允许用户对允许分区的数据访问，同时允许每个允许用户在主数据访问简要表支配的规定参数内变更他们自己的简要表。

本发明的进一步可替代实施例可以采取与数据存储媒体结合执行所有访问控制功能，或取代与像上述 SDV 那样的保密设备结合，与操作系统结合在

一起运行的访问控制应用程序的形式。对于这种安排，在访问控制应用程序控制的主数据访问简要表和当前数据访问简要表的限定内，通过操作系统实现对驱动器和/或分区的访问许可或拒绝。

本发明的更进一步实施例可以采取可与计算系统连接和包含适当软件使访问控制系统与操作系统、SDV 型保密设备、或任何其它适当访问控制安排结合在一起运行的硬件实现访问控制系统的形式。

在允许在系统管理者或超级用户确定的限制内对预定用户进行分区访问控制方面本发明提供的一些优点如下:

>系统管理者完全控制了可以由访问控制应用程序控制的用户和分区。

>每个用户只需要一个简要表在启动时用于验证。

>用户必须记住的通行字个数最少。

>为了保护数据存储器上的数据，用户可以在正常系统操作期间的任何时候，在它们的允许控制范围内变更那些分区的读或写访问许可。

>用户可以不关掉电源地禁止对所有分区的访问，使它们离开计算机处在保密状态下。第三方必须知道允许用户通行字才能够访问禁止分区。

>访问控制应用程序可以通过 CD 分发或从因特网上提供的网站中下载。

>访问控制应用程序可以存储在 HDD 上的加密“只读”分区中，以便有助于保持系统完整性。

在本发明的方法和系统可以用应用软件实现，或部分用软件实现的情况下，它们可以采取存储在像 CD-ROM 那样的计算机可读媒体或任何其它机器可读媒体中或可从这样的计算机可读媒体中获得的程序代码的形式，程序代码包含当被装入像计算机那样的机器中时，使机器变成实现本发明的系统的指令。计算机可读媒体可以包括像光缆那样的媒体或任何其它形式的传输媒体。

应该体会到，本发明不局限于本文所述的特定实施例。于是，在不偏离本发明的精神和范围的情况下，可以根据传统软件和计算机工程实践设想出最佳方式的可替代实施例和变体。

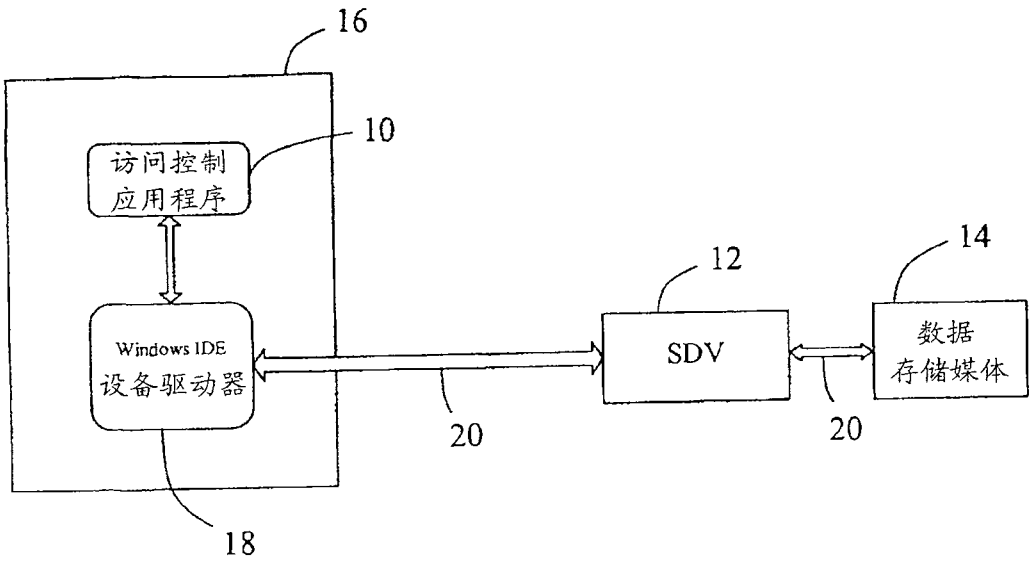


图 1

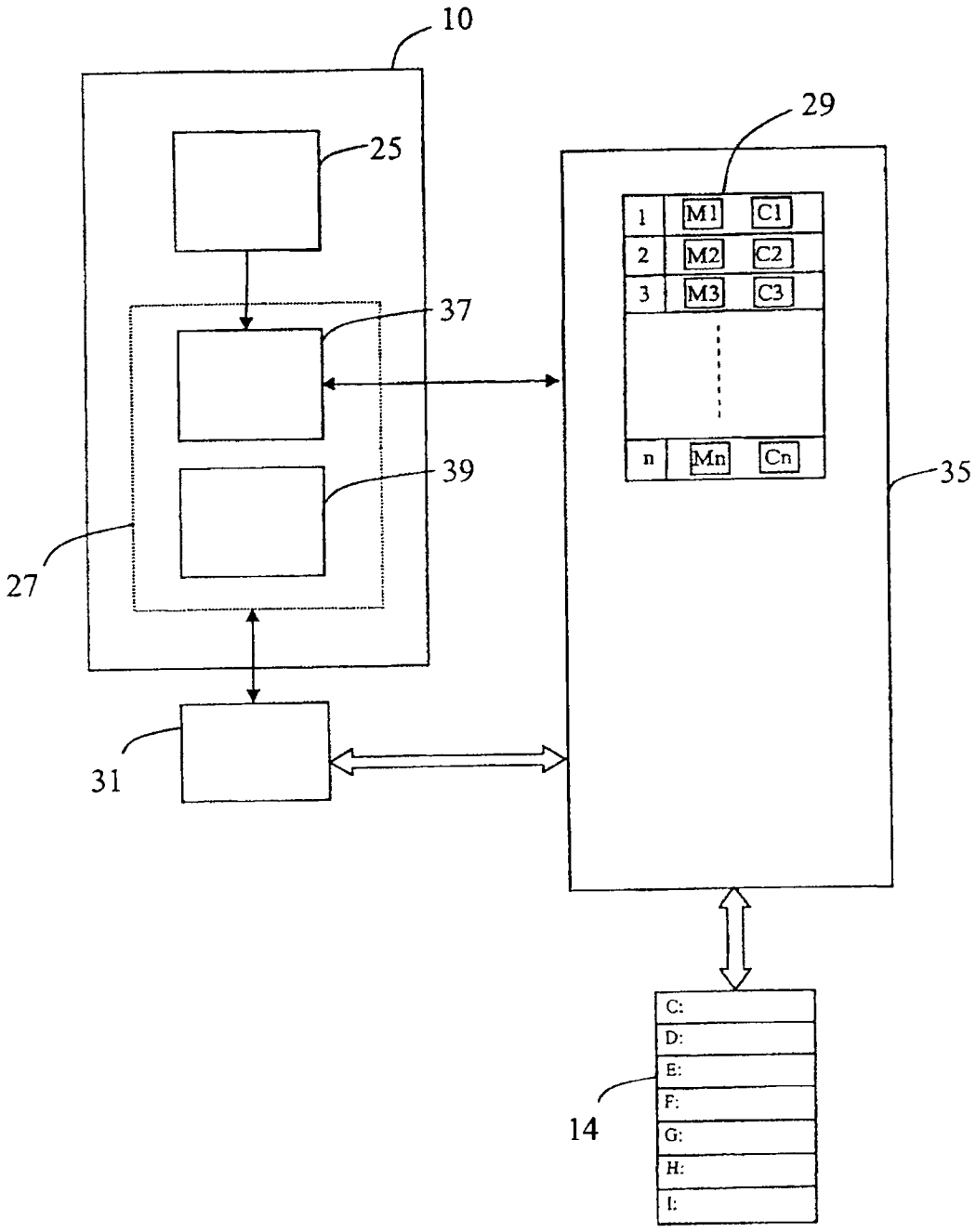


图 2

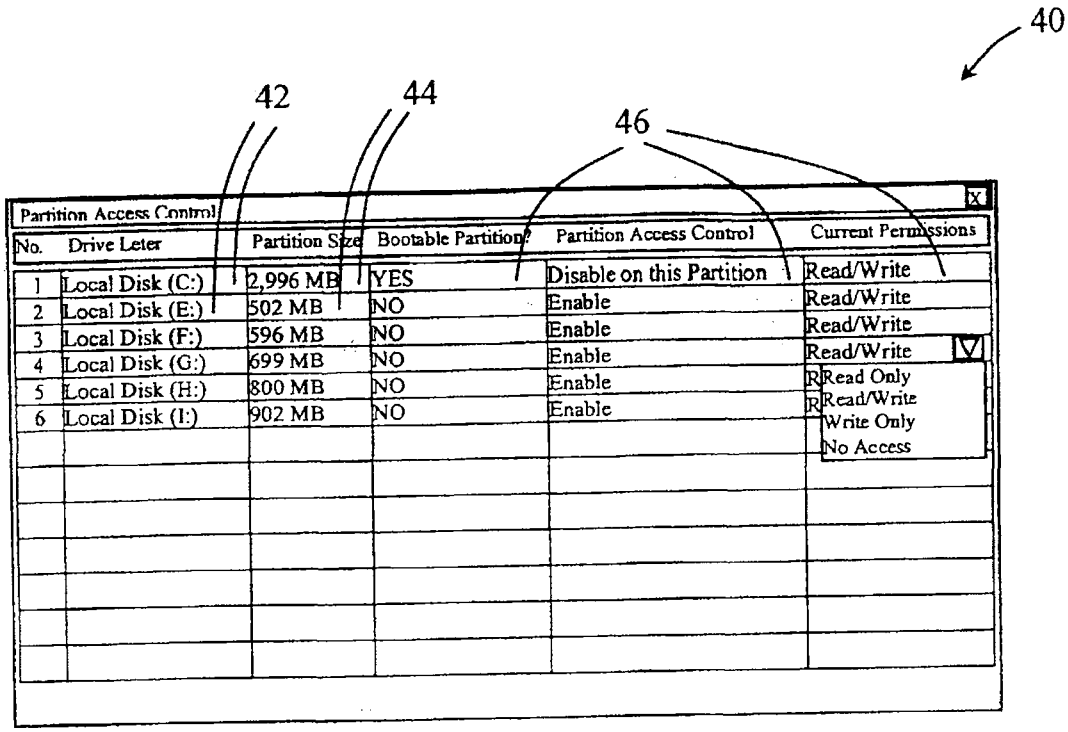

40
42
44
46
Partition Access Control
No.
Drive Leter
Partition Size
Bootable Partition?
Partition Access Control
Current Permissions
1 Local Disk (C:) 2,996 MB YES Disable on this Partition Read/Write
2 Local Disk (E:) 502 MB NO Enable Read/Write
3 Local Disk (F:) 596 MB NO Enable Read/Write
4 Local Disk (G:) 699 MB NO Enable Read/Write
5 Local Disk (H:) 800 MB NO Enable
6 Local Disk (I:) 902 MB NO Enable
Read Only
Read/Write
Write Only
No Access

图 3

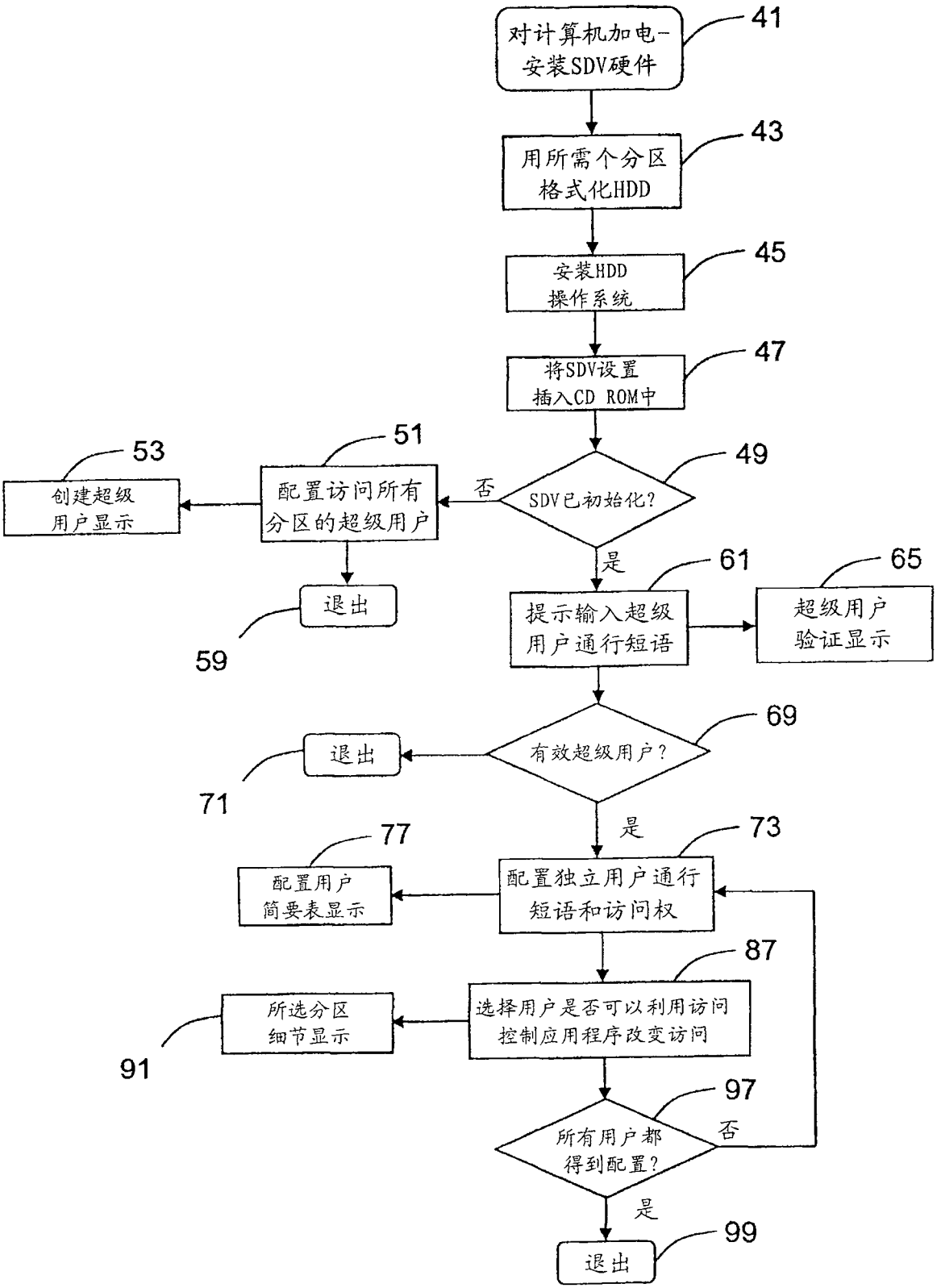

对计算机加电-安装SDV硬件
41
用所需个分区格式化HDD
43
安装HDD操作系统
45
将SDV设置插入CD ROM中
47
SDV已初始化?
49
否
是
配置访问所有分区的超级用户
51
创建超级用户显示
53
退出
59
提示输入超级用户通行短语
61
超级用户验证显示
65
有效超级用户?
69
退出
71
是
配置独立用户通行短语和访问权
73
配置用户简要表显示
77
选择用户是否可以利用访问控制应用程序改变访问
87
所选分区细节显示
91
所有用户都得到配置?
97
否
是
退出
99

图 4

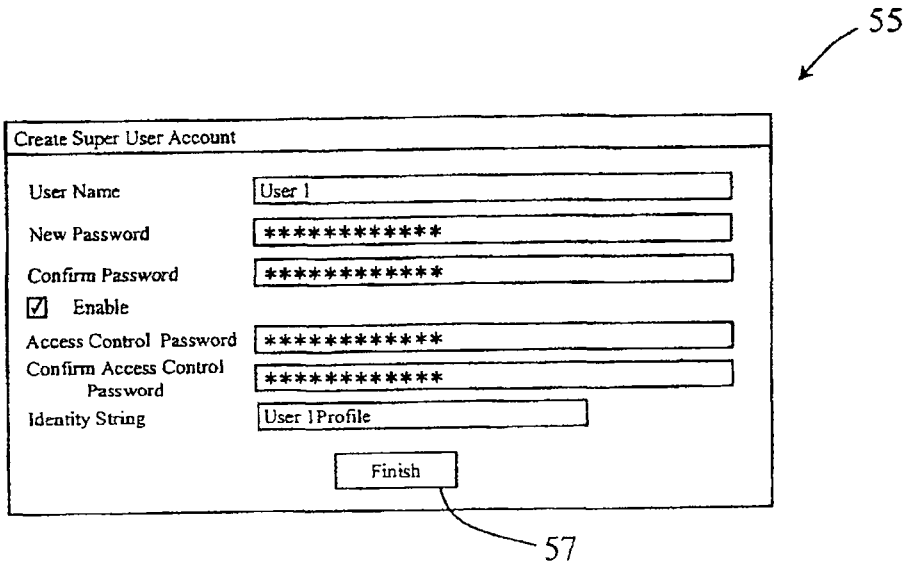

55
Create Super User Account
User Name
User 1
New Password
****
Confirm Password
****
Enable
Access Control Password
****
Confirm Access Control Password
****
Identity String
User 1Profile
Finish
57

图 5

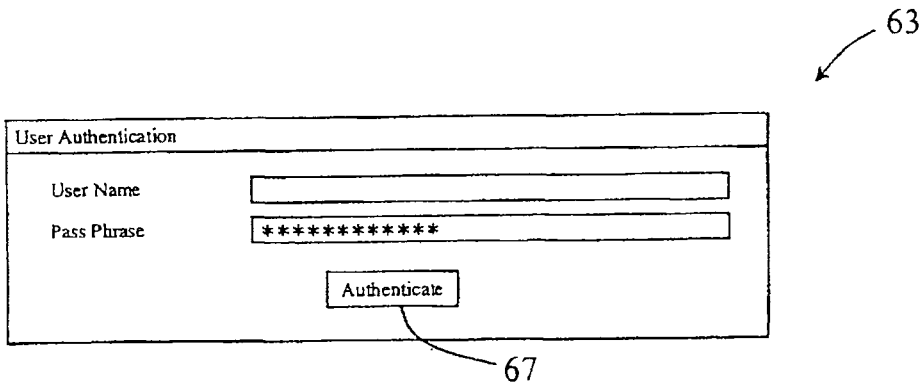

63
User Authentication
User Name
Pass Phrase
****
Authenticate
67

图 6

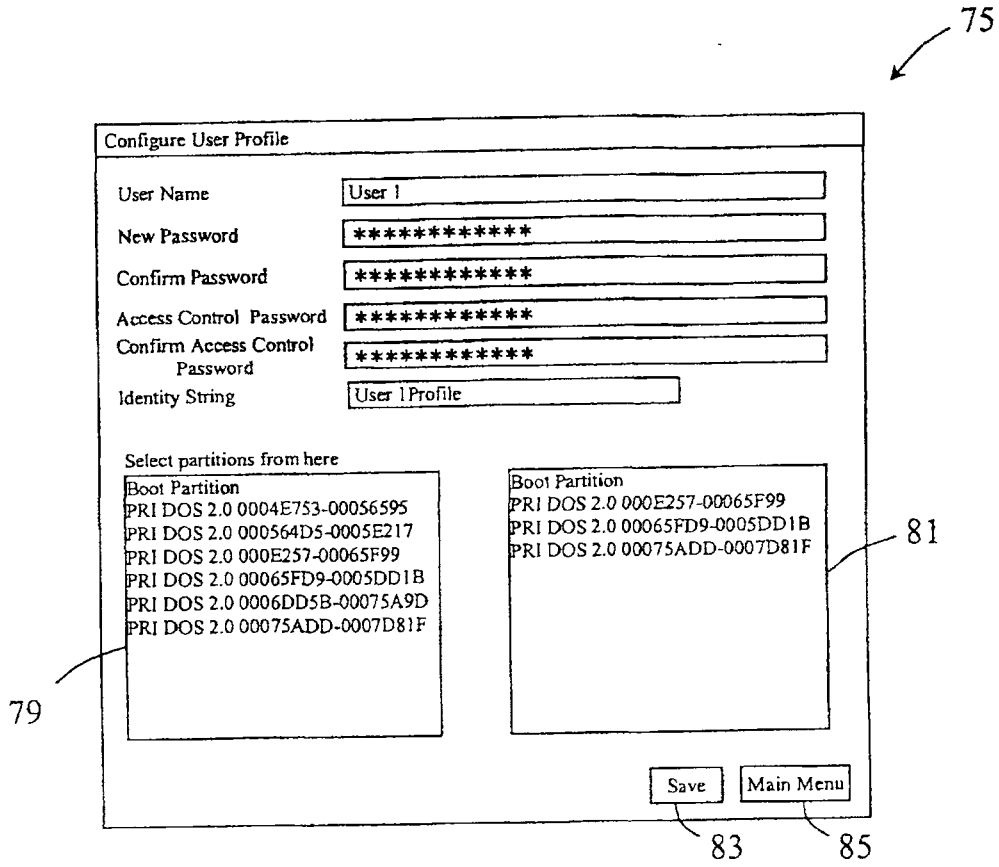

75
Configure User Profile
User Name
User 1
New Password
****
Confirm Password
****
Access Control Password
****
Confirm Access Control Password
****
Identity String
User 1Profile
Select partitions from here
Boot Partition
PRI DOS 2.0 0004E753-00056595
PRI DOS 2.0 000564D5-0005E217
PRI DOS 2.0 000E257-00065F99
PRI DOS 2.0 00065FD9-0005DD1B
PRI DOS 2.0 0006DD5B-00075A9D
PRI DOS 2.0 00075ADD-0007D81F
Boot Partition
PRI DOS 2.0 000E257-00065F99
PRI DOS 2.0 00065FD9-0005DD1B
PRI DOS 2.0 00075ADD-0007D81F
81
79
Save
Main Menu
83
85

图 7

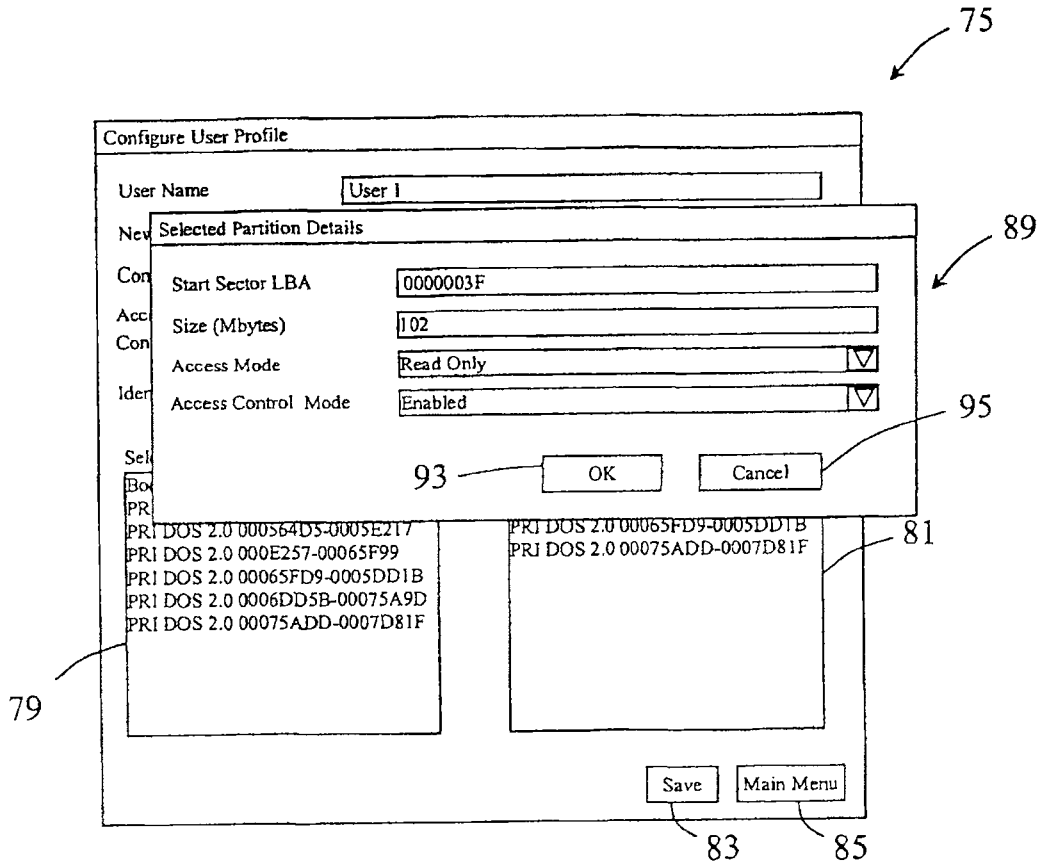

75
Configure User Profile
User Name
User 1
Selected Partition Details
89
Start Sector LBA
0000003F
Size (Mbytes)
102
Access Mode
Read Only
Access Control Mode
Enabled
95
93
OK
Cancel
PRI DOS 2.0 000564D5-0005E217
PRI DOS 2.0 000E257-00065F99
PRI DOS 2.0 00065FD9-0005DD1B
PRI DOS 2.0 0006DD5B-00075A9D
PRI DOS 2.0 00075ADD-0007D81F
PRI DOS 2.0 00065FD9-0005DD1B
PRI DOS 2.0 00075ADD-0007D81F
81
79
Save
Main Menu
83
85

图 8

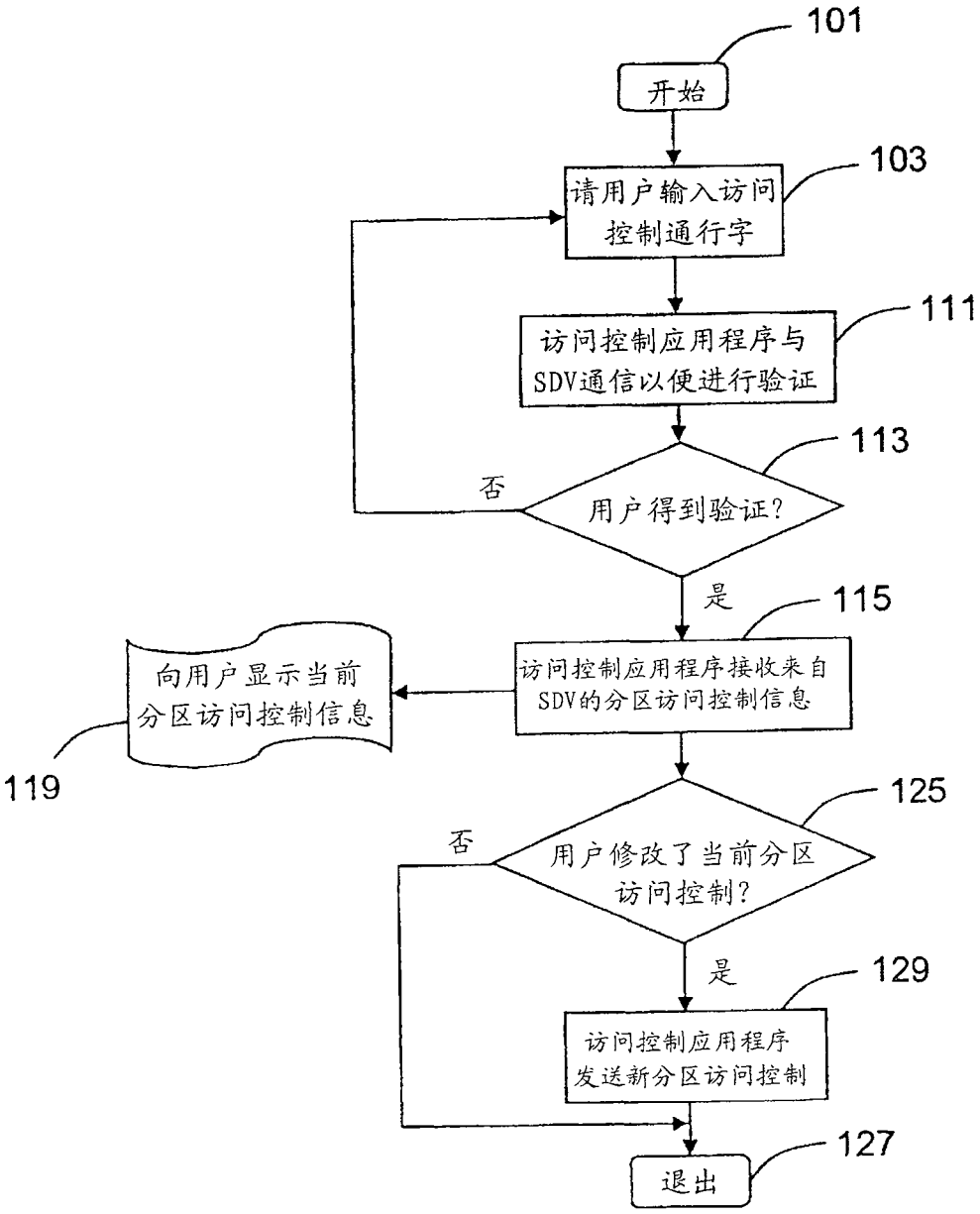

101
开始
103
请用户输入访问控制通行字
111
访问控制应用程序与SDV通信以便进行验证
113
否
用户得到验证?
是
115
访问控制应用程序接收来自SDV的分区访问控制信息
向用户显示当前分区访问控制信息
119
125
否
用户修改了当前分区访问控制?
是
129
访问控制应用程序发送新分区访问控制
127
退出

图 9

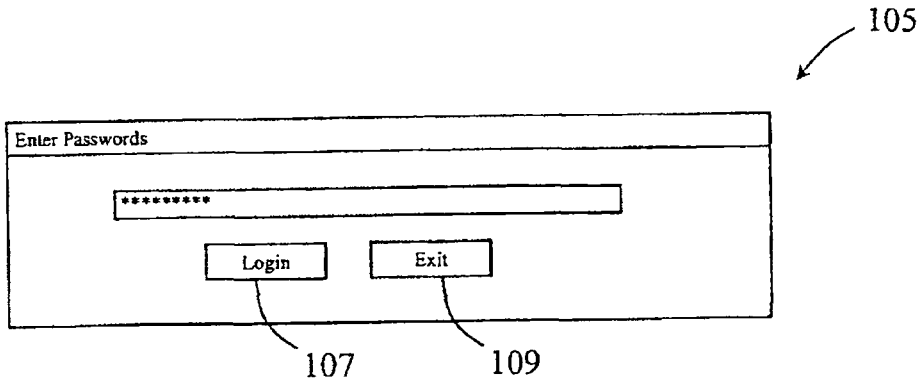

105
Enter Passwords
****
Login
Exit
107
109

图 10

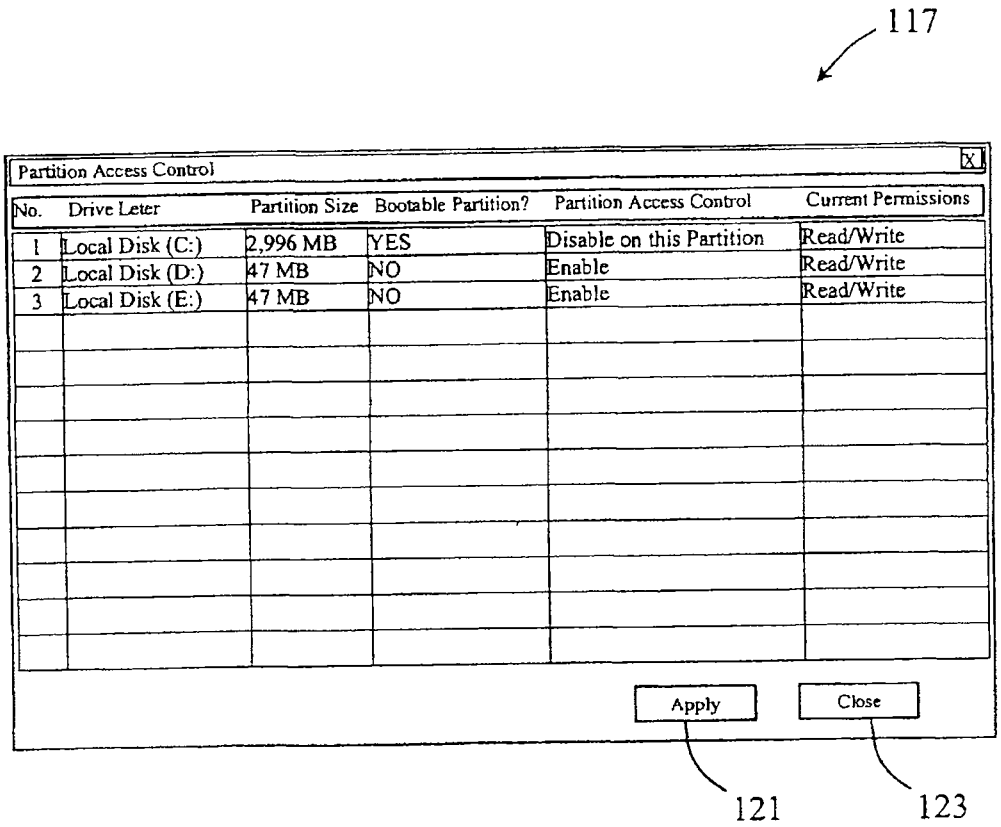

117
Partition Access Control
No.
Drive Leter
Partition Size
Bootable Partition?
Partition Access Control
Current Permissions
1 Local Disk (C:) 2,996 MB YES Disable on this Partition Read/Write
2 Local Disk (D:) 47 MB NO Enable Read/Write
3 Local Disk (E:) 47 MB NO Enable Read/Write
Apply
Close
121
123

图 11

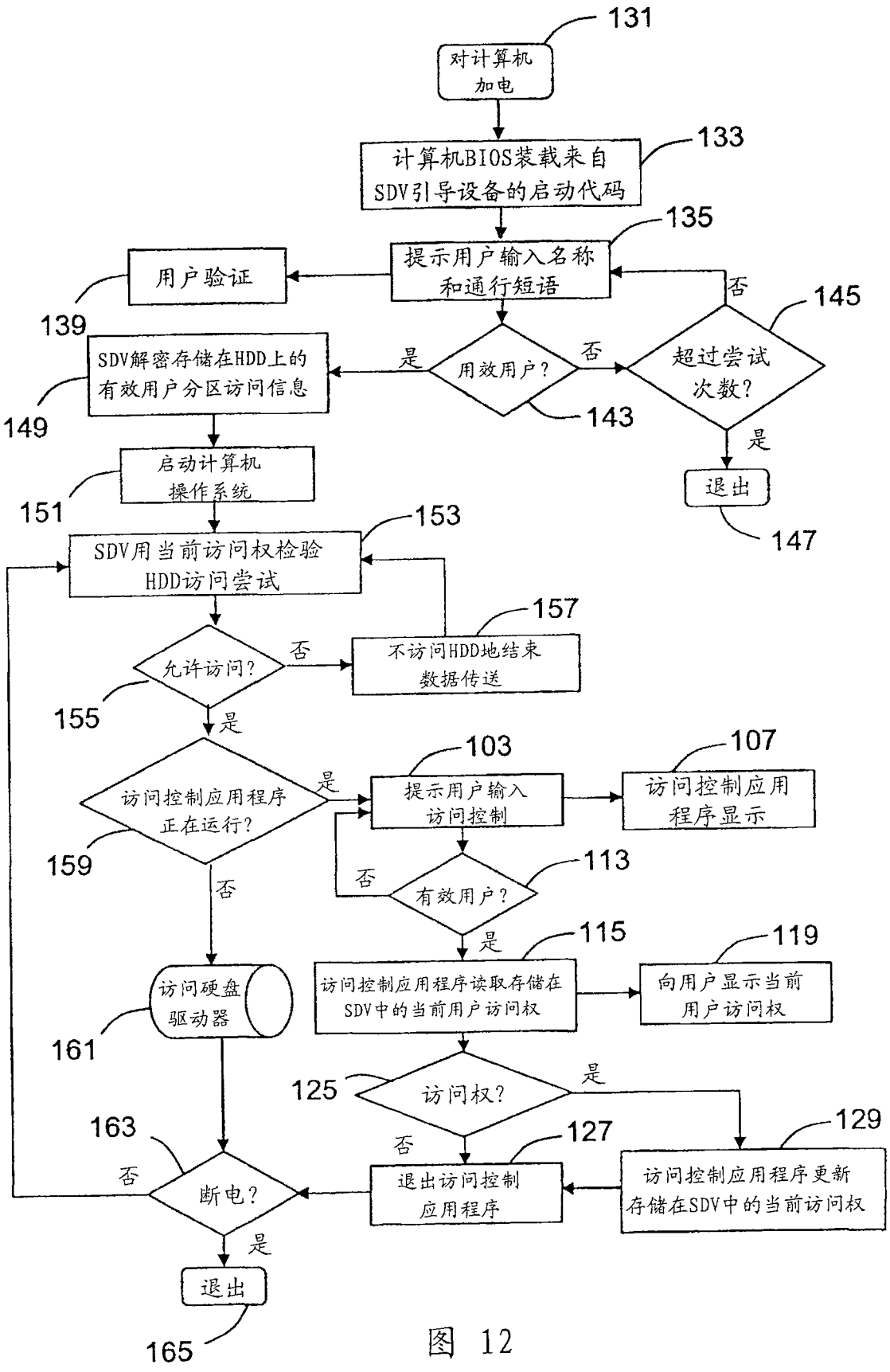

131
对计算机加电
133
计算机BIOS装载来自SDV引导设备的启动代码
135
提示用户输入名称和通行短语
用户验证
139
SDV解密存储在HDD上的有效用户分区访问信息
149
是
用效用户?
否
143
否
超过尝试次数?
145
是
退出
147
启动计算机操作系统
151
SDV用当前访问权检验HDD访问尝试
153
允许访问?
否
不访问HDD地结束数据传送
157
155
是
访问控制应用程序正在运行?
159
是
103
提示用户输入访问控制
107
访问控制应用程序显示
否
有效用户?
113
否
是
115
访问控制应用程序读取存储在SDV中的当前用户访问权
119
向用户显示当前用户访问权
访问硬盘驱动器
161
125
访问权?
是
否
127
129
访问控制应用程序更新存储在SDV中的当前访问权
退出访问控制应用程序
163
否
断电?
是
退出
165

图 12

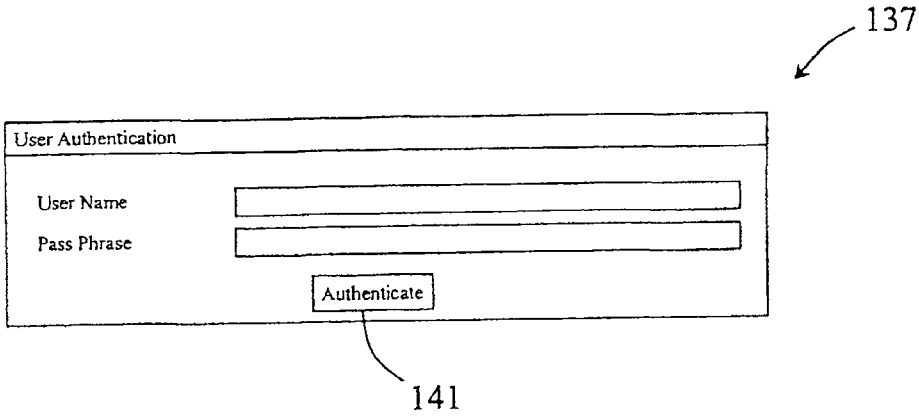

137
User Authentication
User Name
Pass Phrase
Authenticate
141

图 13