

基于虚拟化的可信计算度量方法、装置、设备和存储介质

5 本申请要求于 2022 年 03 月 03 日提交中国专利局、申请号为 202210202759.2、申请名称为“基于虚拟化的可信计算度量方法、装置、设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

10 本申请实施例涉及计算机技术领域，特别是涉及一种基于虚拟化的可信计算度量方法和装置、一种电子设备和一种存储介质。

背景技术

机密计算（Confidential Computing，也译作保密计算/可信计算）是通过基于硬件的可信执行环境（TEE，Trusted Execution Environment）对使用中的数据进行保护。TEE 被定义为提供一定级别的数据完整性、数据机密性和代码完整性保证的环境。

15 目前，可以将应用程序（Application，App）作为度量对象进行可信计算度量，进而确定是否允许该应用程序在可信执行环境中运行，然而，目前的技术方案只能对应用程序进行整体的可信计算度量，无法对应用程序进行细粒度的可信计算度量，进而更好地基于应用程序提供服务。

发明内容

20 本申请实施例提供了一种基于虚拟化的可信计算度量方法，以解决无法对应用程序进行细粒度的可信计算度量的问题。

相应的，本申请实施例还提供了一种基于虚拟化的可信计算度量装置、一种电子设备以及一种存储介质，用以保证上述方法的实现及应用。

25 为了解决上述问题，本申请实施例公开了一种基于虚拟化的可信计算度量方法，所述方法包括：

确定待度量的应用程序；

从所述应用程序中分离出目标度量数据，并将所述目标度量数据存储至虚拟机的虚拟镜像文件中，所述虚拟机中包括可信执行环境；

确定加载至所述可信执行环境的目标虚拟镜像文件的可信程度；

30 根据所述目标虚拟镜像文件的所述可信程度，允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

可选地，所述目标度量数据包括应用程序的代码、配置文件和环境变量。

可选地，所述确定加载至所述可信执行环境的目标虚拟镜像文件的可信程度，包括：采用指定摘要算法计算加载至所述可信执行环境的目标虚拟镜像文件的度量值，所述

度量值用于表征所述虚拟镜像文件的可信程度；

将所述目标虚拟镜像文件的度量值写入所述虚拟机的指定存储区域中；所述指定存储区域在所述可信执行环境中运行过程中禁止写入。

- 5 可选地，所述根据所述目标虚拟镜像文件的所述可信程度，允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行，包括：

在所述可信执行环境运行过程中，从所述指定存储区域中读取所述目标虚拟镜像文件的度量值；

将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

- 10 可选地，所述将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行，包括：

当所述目标虚拟镜像文件的度量值与黑名单中的预设度量值匹配时，禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行；

- 15 当所述目标虚拟镜像文件的度量值与白名单中的预设度量值匹配时，运行所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

可选地，在所述将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行之前，所述方法还包括：

- 20 确定服务级别，从所述配置文件中获取所述服务级别对应的预设度量值。

可选地，所述方法还包括：

在所述可信执行环境运行结束时，销毁所述指定存储区域中的所述度量值。

本申请实施例还公开了一种基于虚拟化的可信计算度量装置，所述装置包括：

应用程序确定模块，用于确定待度量的应用程序；

- 25 数据分离模块，用于从所述应用程序中分离出目标度量数据，并将所述目标度量数据存储至虚拟机的虚拟镜像文件中，所述虚拟机中包括可信执行环境；

可信程度确定模块，用于确定加载至所述可信执行环境的目标虚拟镜像文件的可信程度；

- 30 可信程度判断模块，用于根据所述目标虚拟镜像文件的所述可信程度，允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

可选地，所述目标度量数据包括应用程序的代码、配置文件和环境变量。

- 35 可选地，所述可信程度确定模块，用于采用指定摘要算法计算加载至所述可信执行环境的目标虚拟镜像文件的度量值，所述度量值用于表征所述虚拟镜像文件的可信程度；将所述目标虚拟镜像文件的度量值写入所述虚拟机的指定存储区域中；所述指定存储区域在所述可信执行环境中运行过程中禁止写入。

可选地，所述可信程度判断模块，用于在所述可信执行环境运行过程中，从所述指定存储区域中读取所述目标虚拟镜像文件的度量值；将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

5 可选地，所述可信程度判断模块，用于当所述目标虚拟镜像文件的度量值与黑名单中的预设度量值匹配时，禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行；当所述目标虚拟镜像文件的度量值与白名单中的预设度量值匹配时，运行所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

10 可选地，所述装置还包括：服务级别确定模块，用于确定服务级别，从所述配置文件中获取所述服务级别对应的预设度量值。

可选地，所述装置还包括：销毁模块，用于在所述可信执行环境运行结束时，销毁所述指定存储区域中的所述度量值。

15 本申请实施例还公开了一种电子设备，包括：处理器；和存储器，其上存储有可执行代码，当所述可执行代码被执行时，使得所述处理器执行如本申请实施例中一个或多个所述的基于虚拟化的可信计算度量方法。

本申请实施例还公开了一个或多个机器可读介质，其上存储有可执行代码，当所述可执行代码被执行时，使得处理器执行如本申请实施例中一个或多个所述的基于虚拟化的可信计算度量方法。

20

与现有技术相比，本申请实施例包括以下优点：

在本申请实施例中，从待度量的应用程序分离出目标度量数据，并将目标度量数据分别存储至虚拟机的虚拟镜像文件中，然后，在将目标虚拟镜像文件加载至虚拟机的可信执行环境后，确定目标虚拟镜像文件的可信程度，以基于可信程度允许或者禁止目标虚拟镜像文件对应的应用程序在可信执行环境中运行。本申请实施例可以对应用程序进行细粒度的可信计算度量，进而可以基于细粒度的度量结果更好地提供服务。

25

附图说明

图 1 是本申请的一种基于虚拟化的可信计算度量方法实施例的步骤流程图；

图 2 是本申请的一种应用程序打包至镜像文件的示意图；

30 图 3 是本申请的另一种基于虚拟化的可信计算度量方法实施例的步骤流程图；

图 4 是本申请的一组协同工作的应用程序的可信计算度量示意图；

图 5 是本申请的一种基于虚拟化的可信计算度量步骤流程图；

图 6 是本申请的一种基于虚拟化的可信计算度量装置实施例的结构框图；

图 7 是本申请一实施例提供的装置的结构示意图。

35 **具体实施方式**

为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

首先，对于本申请实施例涉及的一些技术名词进行说明：

TEE: Trusted Execution Environment, 可信执行环境；

5 SEV: Secure Memory Encryption, 一种基于虚拟化的 TEE 技术；

TDX: Trust Domain Extensions, 一种基于虚拟化的 TEE 技术；

TPM : Trusted Platform Module, 可信平台模块。

在具体实现中，DataTrust(隐私增强计算平台) 是一种基于可信执行环境的安全产品，用户将数据以加密形式导入运行在 TEE 中的数据计算引擎执行计算，然后将运算结果以加密形式再返回给用户。TEE 用来保护数据计算引擎，确保应用程序符合预期，且不会因为外部的攻击者或恶意管理员攻击而被篡改。

典型的基于虚拟化的机密计算执行环境 TEE 技术如 SEV、TDX，利用硬件保护虚拟机运行时所使用的内存，使除虚拟机用户之外的任何人都无法对其进行访问。具体地，虚拟机软件将系统内核、中间件以及应用程序和数据打包在一起生成虚拟磁盘镜像文件，虚拟机在启动后加载该镜像文件，读写位于其中的程序和数据。上述技术方案在应用于 TEE 时通常难以发挥其能力，这是由于每次虚拟机运行都会修改镜像文件，如果将镜像文件作为 TEE 的度量对象，会导致度量对象的度量值随时变化且难以预测，因而无法将镜像文件的度量值作为判断依据。

此外，还有基于 TPM 方案和 Kata Containers 方案，其中，基于 TPM 的方案，基于 TPM 的应用程序的度量能力 (IMA)，以应用程序的内的每个二进制文件 (代码) 为度量对象进行度量，并根据度量结果决定是否允许执行，该方案无法体现度量对象的逻辑关系；基于 Kata Containers 方案，利用虚拟机承载容器实例运行的容器运行时，但无法为容器实例提供基于机密计算执行环境的运行时保护。

针对上述问题，本申请实施例提出了一种虚拟化的可信计算度量方法，具体地，从待度量的应用程序分离出目标度量数据，将目标度量数据作为不可变的数据存储至虚拟机的虚拟镜像文件中，然后，将虚拟机的虚拟镜像文件能够作为不变、且可预测的度量对象，进而生成不变、且可预测的度量值作为该虚拟镜像文件的可信程度的判断依据，实现应用程序的细粒度的可信计算度量。需要说明的是，本申请实施例可以将一个应用程序存储至虚拟镜像文件进行可信计算度量，也可以将一组协同工作的应用程序存储至虚拟镜像文件进行可信计算度量，对此不加以限定。

参照图 1，是本申请的一种基于虚拟化的可信计算度量方法实施例的步骤流程图，包括如下步骤：

步骤 102、确定待度量的应用程序。

35 其中，待度量的应用程序可以是一个应用程序，也可以是一组协同工作的应用程序，

本申请实施例对此无需加以限制。举例来说，待度量的应用程序可以是一个应用程序，例如 App1，也可以是一组协同工作的应用程序，例如 App1、App2 和 App3。

步骤 104、从所述应用程序中分离出目标度量数据，并将所述目标度量数据存储至虚拟机的虚拟镜像文件中，所述虚拟机中可以包括可信执行环境。

5 其中，应用程序通常由代码、配置文件、环境变量和持久化存储的数据组成。代码：通常指机器可识别的执行码，例如 C 语言编译后产生的二进制可执行文件、Python 语言编写的.py 脚本；配置文件：通常以文本形式提供，代码在运行时读取该文件并解析配置，会影响代码执行路径；环境变量：通常由操作系统或用户指定，会影响代码执行路径；持久化存储的数据：存储在硬盘等持久化存储设备上的数据，例如数据库文件等等。

10 其中，所述目标度量数据可以包括应用程序的代码、配置文件和环境变量。参照图 2，是本申请的一种应用程序打包至镜像文件的示意图，具体地，从应用程序中分离出代码、配置文件、环境变量和持久化存储的数据（持久化数据）后，将代码、配置文件和环境变量存储至虚拟机的虚拟镜像文件中，以及将持久化存储的数据存储至外部存储设备的磁盘镜像文件中。

15 在本申请实施例中，若待度量的应用程序是一组协同工作的应用程序，则可以将一组协同工作的应用程序分别以独立的形式打包至同一镜像文件内，当然，也可以分别打包生成彼此独立的一组镜像文件，本申请实施例对此不加以限制。

虚拟化是一种在同一台机器（计算机）上可以同时运行多种客户操作系统的技术，虚拟机（Virtual Machine）是虚拟化的一种表现方式。具体地，虚拟机指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。在计算机中创建虚拟机时，需要将实体机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟机都有独立的 CMOS、硬盘和操作系统，可以如同使用实体机一样对虚拟机进行操作。其中，在虚拟机中设置有可信执行环境 TEE，可信的应用程序将被允许在可信执行环境 TEE 中运行。

25 步骤 106、确定加载至所述可信执行环境的目标虚拟镜像文件的可信程度。

其中，可信程度用于衡量是否可以允许虚拟镜像文件对应的应用程序在可信执行环境 TEE 中运行。简单来说，如果可信程度较高，则将允许应用程序在可信执行环境 TEE 中运行，反之，如果可信程度较低，则将禁止应用程序在可信执行环境 TEE 中运行。

30 在本申请实施例中，虚拟机的虚拟镜像文件能够作为不变、且可预测的度量对象，进而生成不变、且可预测的度量值作为可信程度的判断依据。具体地，从虚拟镜像文件中确定出需要加载至可信执行环境的内存的目标虚拟镜像文件，在将目标虚拟镜像文件加载至可信执行环境的内容后，将确定目标虚拟镜像文件的可信程度。

步骤 108、根据所述目标虚拟镜像文件的所述可信程度，允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

35 在本申请实施例中，在确定目标虚拟镜像文件的可信程度后，将基于该可信程度，确

定是否运行目标虚拟镜像文件对应的应用程序在可信执行环境中运行。

例如, 假设有两个应用程序 App1、App2, 将分别从 App1、App2 中分离出代码、配置文件、环境变量和持久化存储的数据, 然后分别将 App1、App2 的代码、配置文件、环境变量作为目标度量数据分别存储到虚拟机的虚拟镜像文件 File1、File2 中, 以及将 App1、App2 的持久化存储的数据分别存储到磁盘镜像文件 File1'、File2' 中。假设基于 App1 的 File1 的可信程度确定为允许在可信执行环境中运行, 基于 App2 的 File2 的可信程度确定为禁止在可信执行环境 TEE 中运行, 那么在启动可信执行环境 TEE 后, 在可信执行环境 TEE 中运行 App1, 其中, 在 App1 可以基于在 File1 中存储的数据在可信执行环境 TEE 中运行, 而在可信执行环境 TEE 在运行期间, 若 App1 需要使用到持久化存储的数据, 例如数据库中的数据, 则可以从 File1' 的该数据库中获取到所需的数据并使用。在 App1 在可信执行环境 TEE 结束运行后, 可以释放在 File1' 中存储的持久化存储的数据, 随后, File1' 中的持久化存储的数据不会有变化。

在上述基于虚拟化的度量方法, 从待度量的应用程序分离出目标度量数据, 并将目标度量数据分别存储至虚拟机的虚拟镜像文件中, 然后, 在将目标虚拟镜像文件加载至虚拟机的可信执行环境后, 确定目标虚拟镜像文件的可信程度, 以基于可信程度允许或者禁止目标虚拟镜像文件对应的应用程序在可信执行环境中运行。本申请实施例可以对应用程序进行细粒度的可信计算度量, 进而可以基于细粒度的度量结果更好地提供服务。

参照图 3, 是本申请的另一种基于虚拟化的可信计算度量方法实施例的步骤流程图, 包括如下步骤:

步骤 302、确定待度量的应用程序。

步骤 304、从所述应用程序中分离出目标度量数据, 并将所述目标度量数据存储至虚拟机的虚拟镜像文件中, 所述虚拟机中包括可信执行环境。

步骤 306、采用指定摘要算法计算加载至所述可信执行环境的目标虚拟镜像文件的度量值, 所述度量值用于表征所述虚拟镜像文件的可信程度。

步骤 308、将所述目标虚拟镜像文件的度量值写入所述虚拟机的指定存储区域中; 所述指定存储区域在所述可信执行环境中运行过程中禁止写入。

其中, 在可信执行环境 TEE 中设置了可信根/信任根 (RoT, Root of Trust), 具体地, 可信根是指一种专用安全硬件、固件或软件组件, 基于可信根可以实现特定安全功能。在本申请实施例中, 为可信根定义了一组接口 (指定存储区域), 寄存器是其中一种可行的实现方式。

作为一个可选示例, 指定摘要算法可以是 SHA256 算法等加密算法。在本申请实施例中, 可信根采用 SHA256 算法对加载至可信执行环境 TEE 的目标虚拟镜像文件计算度量值, 并将度量值写入接口中。需要说明的是, 在到可信执行环境 TEE 运行的过程中, 接口将变成只读不允许写入, 直至结束运行被销毁。

步骤 310、在所述可信执行环境运行过程中，从所述指定存储区域中读取所述目标虚拟镜像文件的度量值。

步骤 312、将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

5 在本申请实施例中，在可信执行环境运行过程中，从指定存储区域中读取目标虚拟镜像文件的度量值，然后，将目标虚拟镜像文件的度量值与预设度量值进行比对，进而根据比对结果允许或者禁止目标虚拟镜像文件对应的应用程序在可信执行环境 TEE 中运行。

在本申请一种可选实施例中，所述步骤 312、将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序
10 在所述可信执行环境中运行，可以包括如下步骤：

当所述目标虚拟镜像文件的度量值与黑名单中的预设度量值匹配时，禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行；

当所述目标虚拟镜像文件的度量值与白名单中的预设度量值匹配时，运行所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

15 在本申请实施例中，可以通过黑白名单机制来判定应用程序的可信程度。应用程序可以将受信任的应用组件（目标度量数据）的度量值作为预设度量值保存到白名单、将不受信任的应用组件的度量值作为作为预设度量值保存到黑名单，黑/白名单作为配置文件的形式打包在镜像文件中。

举例来说，假设应用程序 App1 和 App2 的虚拟镜像文件的度量值为：App1: 123456、
20 App2: 56789，黑名单中的预设度量值为 Digest: 56789，由于，App2 的度量值 56789 与黑名单中的预设度量值 56789 匹配，则可以将度量值为 56789 的 App2 禁止在可信执行环境 TEE 中运行。

步骤 314、在所述可信执行环境运行结束时，销毁所述指定存储区域中的所述度量值。

在本申请实施例中，在到可信执行环境 TEE 运行的过程中，接口将变成只读不允许写入，即，只允许读取其中的度量值但不允许写入其他的度量值，以使在接口中的度量值能够保持不变，直至可信执行环境 TEE 结束运行时，接口或者接口中的度量值可以被销毁。
25

在本申请一种可选实施例中，在所述将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行之前，所述方法还可以包括如下步骤：

30 确定服务级别，从所述配置文件中获取所述服务级别对应的预设度量值。

在具体实现中，通过一个或一组应用程序组成的抽象，可以对外提供一种特定的服务，例如，nginx 服务器提供的 HTTP 服务。

在本申请实施例中，可以根据不同的服务需求确定不同的服务级别，进而基于服务级别从配置文件中获取服务级别对应的预设度量值，用于确定是否允许应用程序在可信执行
35 环境 TEE 中运行，实现不同服务级别的应用可用性保障。

为了使本领域技术人员更好地理解本申请，以下采用具体的示例进行说明。

在相关 TEE 技术方案中，利用可信根生成所度量对象的度量值，无论是 SEV 还是 TDX，都只能度量一个对象。而本申请实施例对可信执行环境 TEE 的可信根进行扩展，使其能够生成足够多、或任意多的且彼此独立的度量结果。在将应用程序的代码、配置文件和环境
5 变量保存至虚拟机的虚拟镜像文件，位于可信执行环境 TEE 内运行的系统能够根据对应的度量值在黑白名单中检查某一应用组件是否被篡改或不被信任，从而使系统能够灵活的运行一个最大的可信任应用集合来提供服务。

本申请实施例为基于虚拟化的机密计算技术提供分段度量能力，解决了现有可信执行环境 TEE 技术只能度量一个度量对象的限制。具体地，本申请实施例结合不可变虚拟机镜像方案，运行在可信执行环境 TEE 中的应用程序能够实现细粒度的黑白名单控制能力，在
10 部分应用程序的镜像文件遭到攻击时，可以通过可信执行环境 TEE 检测，并由系统根据黑白名单判断应用程序的受信任情况，实现不同服务级别的应用可用性保障。

基于 TPM 实现的 Linux IMA 解决方案只能对每个二进制文件匹配，无法将有关联的二进制文件、配置文件、环境变量等作为整体判断，因此其黑/白名单的设计非常复杂且难以使用。而在本申请实施例中，可使用容器承载应用程序，参照图 4，是本申请的一组协
15 同工作的应用程序的度量示意图，即图表示的“App1”、“App2”、“App3”分别代表“容器 1”、“容器 2”、“容器 3”，将一组容器镜像作为内部组件打包在虚拟机镜像内，使运行在虚拟机内的一组容器协同工作作为整体对外提供服务。可信根度量对象为容器镜像，每个容器镜像为黑/白名单的一项进行管理，可据此将应用/服务作为判断依据。本申请实施例可结合
20 云虚拟化 Enclave 使用，将虚拟机镜像运行在受保护的 Enclave 执行环境内，相比 Kata Containers，容器实例运行环境更加安全。

参照图 5，是本申请的一种基于虚拟化的可信计算度量步骤流程图，具体地，为可信根定义了一组接口，寄存器是其中一种可行的实现方式，利用这组接口，管理程序按照如下步骤将加载镜像文件：

25 步骤 1. 将要加载的镜像（目标虚拟镜像文件）写入内存；

步骤 2. 将内存起始物理地址和大小写入指定接口（如，寄存器 1），可信根使用指定摘要算法（例如 SHA256 算法）生成度量值；

步骤 3. 重复步骤 1～步骤 2，将所有需要加载的镜像文件写入内存，并生成一组与之对应的度量值；

30 步骤 4. 启动可信执行环境 TEE，接口将变成只读不允许写入，直至结束运行被销毁。

在镜像文件加载完成后，应用程序可以将受信任的应用组件的度量值作为白名单、将不受信任的应用组件的度量值作为黑名单，黑/白名单作为配置文件的形式打包在镜像文件内。在应用程序运行期间，从可信根读取加载过程生成的一组度量值，分别将内部的应用组件的度量值与对应的寄存器记录的度量值进行比较，若比较结果为在白名单中即允许运行，
35 若比较结果为在黑名单中即禁止运行。

应用本申请实施例具有如下优点：1. 为基于虚拟化的机密执行环境提供分段度量能力；2. 为应用提供面向服务的可信任级别；3. 将一组容器镜像运行在受保护的虚拟机内，提供运行时内存保护；4. 以容器镜像(镜像文件)为度量管理对象，相比使用 TPM 的 Linux IMA 解决方案，在提供细粒度的可信计算度量能力的同时，能够简化对应用组件的管理。

5 需要说明的是，对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请实施例并不受所描述的动作顺序的限制，因为依据本申请实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本申请实施例所必须的。

10

在上述实施例的基础上，本实施例还提供了一种基于虚拟化的可信计算度量装置，应用于终端设备、服务器等电子设备中。

参照图 6，示出了本申请的一种基于虚拟化的可信计算度量装置实施例的结构框图，具体可以包括如下模块：

15 应用程序确定模块 602，用于确定待度量的应用程序；

数据分离模块 604，用于从所述应用程序中分离出目标度量数据，并将所述目标度量数据存储至虚拟机的虚拟镜像文件中，所述虚拟机中包括可信执行环境；

可信程度确定模块 606，用于确定加载至所述可信执行环境的目标虚拟镜像文件的可信程度；

20 可信程度判断模块 608，用于根据所述目标虚拟镜像文件的所述可信程度，允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

在本申请的一种可选实施例中，所述目标度量数据包括应用程序的代码、配置文件和环境变量。

25 在本申请的一种可选实施例中，所述可信程度确定模块 606，用于采用指定摘要算法计算加载至所述可信执行环境的目标虚拟镜像文件的度量值，所述度量值用于表征所述虚拟镜像文件的可信程度；将所述目标虚拟镜像文件的度量值写入所述虚拟机的指定存储区域中；所述指定存储区域在所述可信执行环境中运行过程中禁止写入。

30 在本申请的一种可选实施例中，所述可信程度判断模块 608，用于在所述可信执行环境运行过程中，从所述指定存储区域中读取所述目标虚拟镜像文件的度量值；将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

35 在本申请的一种可选实施例中，所述可信程度判断模块 608，用于当所述目标虚拟镜像文件的度量值与黑名单中的预设度量值匹配时，禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行；当所述目标虚拟镜像文件的度量值与白名单中的预设度量值匹配时，运行所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

在本申请的一种可选实施例中，所述装置还包括：服务级别确定模块，用于确定服务级别，从所述配置文件中获取所述服务级别对应的预设度量值。

在本申请的一种可选实施例中，所述装置还包括：销毁模块，用于在所述可信执行环境运行结束时，销毁所述指定存储区域中的所述度量值。

5 本申请实施例还提供了一种非易失性可读存储介质，该存储介质中存储有一个或多个模块（programs），该一个或多个模块被应用在设备时，可以使得该设备执行本申请实施例中各方法步骤的指令（instructions）。

 本申请实施例提供了一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得电子设备执行如上述实施例中一个或多个所述的方法。本申请实施例中，
10 所述电子设备包括终端设备、服务器（集群）等各类型的设备。

 本公开的实施例可被实现为使用任意适当的硬件，固件，软件，或及其任意组合进行想要的配置的装置，该装置可包括终端设备、服务器（集群）等电子设备。图 7 示意性地示出了可被用于实现本申请中所述的各个实施例的示例性装置 700。

15 对于一个实施例，图 7 示出了示例性装置 700，该装置具有一个或多个处理器 702、被耦合到(一个或多个)处理器 702 中的至少一个的控制模块（芯片组）704、被耦合到控制模块 704 的存储器 706、被耦合到控制模块 704 的非易失性存储器(NVM)/存储设备 708、被耦合到控制模块 704 的一个或多个输入/输出设备 710，以及被耦合到控制模块 704 的网络接口 712。

20 处理器 702 可包括一个或多个单核或多核处理器，处理器 702 可包括通用处理器或专用处理器（例如图形处理器、应用处理器、基频处理器等）的任意组合。在一些实施例中，装置 700 能够作为本申请实施例中所述终端设备、服务器（集群）等设备。

 在一些实施例中，装置 700 可包括具有指令 714 的一个或多个计算机可读介质(例如，存储器 706 或 NVM/ 存储设备 708) 以及与该一个或多个计算机可读介质相合并被配置为
25 执行指令 714 以实现模块从而执行本公开中所述的动作的一个或多个处理器 702。

 对于一个实施例，控制模块 704 可包括任意适当的接口控制器，以向(一个或多个)处理器 702 中的至少一个和/或与控制模块 704 通信的任意适当的设备或组件提供任意适当的接口。

 控制模块 704 可包括存储器控制器模块，以向存储器 706 提供接口。存储器控制器模块可以是硬件模块、软件模块和/或固件模块。
30 存储器 706 可被用于例如为装置 700 加载和存储数据和/或指令 714。对于一个实施例，存储器 706 可包括任意适当的易失性存储器，例如，适当的 DRAM。在一些实施例中，存储器 706 可包括双倍数据速率类型四同步动态随机存取存储器(DDR4SDRAM)。

 对于一个实施例，控制模块 704 可包括一个或多个输入/输出控制器，以向 NVM/存储设备 708 及(一个或多个)输入/输出设备 710 提供接口。
35

例如, NVM/存储设备 708 可被用于存储数据和/或指令 714。NVM/存储设备 708 可包括任意适当的非易失性存储器(例如, 闪存)和/或可包括任意适当的(一个或多个)非易失性存储设备(例如, 一个或多个硬盘驱动器(HDD)、一个或多个光盘(CD) 驱动器和/或一个或多个数字通用光盘(DVD) 驱动器)。

- 5 NVM/存储设备 708 可包括在物理上作为装置 700 被安装在其上的设备的一部分的存储资源, 或者其可被该设备访问可不必作为该设备的一部分。例如, NVM/存储设备 708 可通过网络经由(一个或多个)输入/输出设备 710 进行访问。

- (一个或多个)输入/输出设备 710 可为装置 700 提供接口以与任意其他适当的设备通信, 输入/输出设备 710 可以包括通信组件、音频组件、传感器组件等。网络接口 712 可为
10 装置 700 提供接口以通过一个或多个网络通信, 装置 700 可根据一个或多个无线网络标准和/或协议中的任意标准和/或协议来与无线网络的一个或多个组件进行无线通信, 例如接入基于通信标准的无线网络, 如 WiFi、2G、3G、4G、5G 等, 或它们的组合进行无线通信。

- 对于一个实施例, (一个或多个)处理器 702 中的至少一个可与控制模块 704 的一个或多个控制器(例如, 存储器控制器模块)的逻辑封装在一起。对于一个实施例, (一个或多个)处理器 702 中的至少一个可与控制模块 704 的一个或多个控制器的逻辑封装在一起以形成系统级封装(SiP)。对于一个实施例, (一个或多个)处理器 702 中的至少一个可与控制模块 704 的一个或多个控制器的逻辑集成在同一模具上。对于一个实施例, (一个或多个)处理器 702 中的至少一个可与控制模块 704 的一个或多个控制器的逻辑集成在同一模具上
15 以形成片上系统(SoC)。

- 在各个实施例中, 装置 700 可以但不限于是: 服务器、台式计算设备或移动计算设备(例如, 膝上型计算设备、手持计算设备、平板电脑、上网本等)等终端设备。在各个实施例中, 装置 700 可具有更多或更少的组件和/或不同的架构。例如, 在一些实施例中, 装置 700 包括一个或多个摄像机、键盘、液晶显示器(LCD) 屏幕(包括触屏显示器)、非易失性存储器端口、多个天线、图形芯片、专用集成电路(ASIC) 和扬声器。
25

其中, 检测装置中可采用主控芯片作为处理器或控制模块, 传感器数据、位置信息等存储到存储器或 NVM/存储设备中, 传感器组可作为输入/输出设备, 通信接口可包括包括网络接口。

- 对于装置实施例而言, 由于其与方法实施例基本相似, 所以描述的比较简单, 相关之处参见方法实施例的部分说明即可。
30

本说明书中的各个实施例均采用递进的方式描述, 每个实施例重点说明的都是与其他实施例的不同之处, 各个实施例之间相同相似的部分互相参见即可。

- 本申请实施例是参照根据本申请实施例的方法、终端设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这
35

些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程基于虚拟化的度量终端设备的处理器以产生一个机器，使得通过计算机或其他可编程基于虚拟化的度量终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

- 5 这些计算机程序指令也可存储在能引导计算机或其他可编程基于虚拟化的度量终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

- 10 这些计算机程序指令也可装载到计算机或其他可编程基于虚拟化的可信计算度量终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

- 15 尽管已描述了本申请实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

- 20 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

- 25 以上对本申请所提供的一种基于虚拟化的可信计算度量方法和装置，一种电子设备和一种存储介质，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

- 1、一种基于虚拟化的可信计算度量方法，其特征在于，所述方法包括：
确定待度量的应用程序；
从所述应用程序中分离出目标度量数据，并将所述目标度量数据存储至虚拟机的虚拟
5 镜像文件中，所述虚拟机中包括可信执行环境；
确定加载至所述可信执行环境的目标虚拟镜像文件的可信程度；
根据所述目标虚拟镜像文件的所述可信程度，允许或者禁止所述目标虚拟镜像文件对
应的应用程序在所述可信执行环境中运行。
- 2、根据权利要求 1 所述的方法，其特征在于，所述目标度量数据包括应用程序的代
10 码、配置文件和环境变量。
- 3、根据权利要求 1 或 2 所述的方法，其特征在于，所述确定加载至所述可信执行环
境的目标虚拟镜像文件的可信程度，包括：
采用指定摘要算法计算加载至所述可信执行环境的目标虚拟镜像文件的度量值，所述
度量值用于表征所述虚拟镜像文件的可信程度；
15 将所述目标虚拟镜像文件的度量值写入所述虚拟机的指定存储区域中；所述指定存储
区域在所述可信执行环境中运行过程中禁止写入。
- 4、根据权利要求 3 所述的方法，其特征在于，所述根据所述目标虚拟镜像文件的所
述可信程度，允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境
中运行，包括：
20 在所述可信执行环境运行过程中，从所述指定存储区域中读取所述目标虚拟镜像文件
的度量值；
将所述目标虚拟镜像文件的度量值与预设度量值进行比对，以根据比对结果允许或者
禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。
- 5、根据权利要求 4 所述的方法，其特征在于，所述将所述目标虚拟镜像文件的度量
25 值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对应
的应用程序在所述可信执行环境中运行，包括：
当所述目标虚拟镜像文件的度量值与黑名单中的预设度量值匹配时，禁止所述目标虚
拟镜像文件对应的应用程序在所述可信执行环境中运行；
当所述目标虚拟镜像文件的度量值与白名单中的预设度量值匹配时，运行所述目标虚
30 拟镜像文件对应的应用程序在所述可信执行环境中运行。
- 6、根据权利要求 4 所述的方法，其特征在于，在所述将所述目标虚拟镜像文件的度
量值与预设度量值进行比对，以根据比对结果允许或者禁止所述目标虚拟镜像文件对
应的应用程序在所述可信执行环境中运行之前，所述方法还包括：
确定服务级别，从所述配置文件中获取所述服务级别对应的预设度量值。
- 35 7、根据权利要求 3 所述的方法，其特征在于，所述方法还包括：

在所述可信执行环境运行结束时，销毁所述指定存储区域中的所述度量值。

8、一种基于虚拟化的可信计算度量装置，其特征在于，所述装置包括：

应用程序确定模块，用于确定待度量的应用程序；

数据分离模块，用于从所述应用程序中分离出目标度量数据，并将所述目标度量数据

5 存储至虚拟机的虚拟镜像文件中，所述虚拟机中包括可信执行环境；

可信程度确定模块，用于确定加载至所述可信执行环境的目标虚拟镜像文件的可信程度；

可信程度判断模块，用于根据所述目标虚拟镜像文件的所述可信程度，允许或者禁止所述目标虚拟镜像文件对应的应用程序在所述可信执行环境中运行。

10

9、一种电子设备，其特征在于，包括：处理器；和

存储器，其上存储有可执行代码，当所述可执行代码被执行时，使得所述处理器执行如权利要求 1-7 中一个或多个所述的基于虚拟化的可信计算度量方法。

10、一个或多个机器可读介质，其上存储有可执行代码，当所述可执行代码被执行时，

15 使得处理器执行如权利要求 1-7 中一个或多个所述的基于虚拟化的可信计算度量方法。