

数据处理系统、方法和存储介质

5 本申请要求于 2022 年 01 月 24 日提交中国专利局、申请号为 202210076690.3、申请名称为“数据处理系统、方法和存储介质”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

本发明涉及计算机领域，具体而言，涉及一种数据处理系统、方法和存储介质。

背景技术

10 在相关技术中，智能板卡中的可信平台控制模块（Trusted Platform Control Module，简称为 TPCM）无法在服务器启动前完成对服务器中的存放启动程序的存储（Boot Rom）和基板管理控制器（BMC Flash）度量，因而额外引入了串行外设接口（Serial Peripheral Interface，简称为 SPI）控制线缆，但额外串行外设接口链路增加了智能网卡上输入/输出的使用量，增加资源消耗，且存在信号质量问题等，从而存在对服务器进行可信度量的效率低的技术问题。

15 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

本发明实施例提供了一种数据处理系统、方法和存储介质，以至少解决对服务器进行可信度量的效率低的技术问题。

20 根据本发明实施例的一个方面，提供了一种数据处理系统。该系统可以包括：服务器和智能板卡，服务器与智能板卡通过高速串行总线 PCIE 物理连线连接，服务器内置串行外设接口总线 SPI，其中，服务器，用于在上电且可信的情况下，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据；其中，智能板卡用于获取服务器通过 SPI 发送，且通过 PCIE 物理连线传输的目标数据，对目标数据进行可信度量，得到度量结果；其中，服务器用于在度量结果表示服务器可信的情况下，将 SPI 切换至 PCIE，且通过 PCIE 进行数据传输。

30 根据本发明实施例的另一方面，还提供了一种数据处理方法。该方法可以包括：响应于智能板卡上电且可信，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，其中，SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据；获取服务器通过内置的串行外设接口总线 SPI 发送，且通过 PCIE 物理连线传输的

目标数据；对目标数据进行可信度量，得到度量结果，其中，在度量结果表示服务器可信时，SPI 由服务器切换至 PCIE，且服务器通过 PCIE 进行数据传输。

根据本发明实施例的另一方面，还提供了一种数据处理装置。该装置可以包括：第一切换单元，用于响应于智能板卡上电且可信，将智能板卡的 PCIE 接口模块切换到智能板卡
5 卡的 SPI 可信度量接口模块，其中，SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据；第一获取单元，用于获取服务器通过内置的串行外设接口总线 SPI 发送，且通过 PCIE 物理连线传输的目标数据；第二切换单元，用于对目标数据进行可信度量，得到度量结果，其中，在度量结果表示服务器可信时，SPI 由服务器切换至 PCIE，且服务器通过 PCIE 进行数据传输。

10 根据本发明实施例的另一方面，还提供了一种计算机可读存储介质，计算机可读存储介质包括存储的程序，其中，在程序运行时控制存储介质所在设备执行上述任意一项的数据处理的方法。

根据本发明实施例的另一方面，还提供了一种处理器，处理器用于运行程序，其中，程序运行时执行上述任意一项的数据处理方法。

15 在本发明实施例中，数据处理系统可以包括服务器和智能板卡，服务器与智能板卡通过高速串行总线 PCIE 物理连线连接，服务器内置串行外设接口总线 SPI，其中，服务器，用于在上电且可信的情况下，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据；其中，智能板卡用于获取服务器通过 SPI 发送，且通过 PCIE 物理连线传输的目标数
20 据，对目标数据进行可信度量，得到度量结果；其中，服务器用于在度量结果表示服务器可信的情况下，将 SPI 切换至 PCIE，且通过 PCIE 进行数据传输。也就是说，本发明通过对服务器的 PCIE 物理连线分时复用，完成服务器启动前的可信度量，不需要额外增加串行外设接口线缆，从而达到了提高对服务器进行可信度量的效率的技术效果，解决了对服务器进行可信度量的效率低的技术问题。

25 附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

图 1 是根据本发明实施例的一种数据处理系统的示意图；

图 2 是根据本发明实施例的一种数据处理方法的计算机终端（或移动设备）的硬件结
30 构框图；

图 3 是根据本发明实施例的一种数据处理方法的流程图；

图 4 是根据本发明相关技术中的一种存在两个可信平台控制模块可信模块的服务器的

示意图;

图 5 是根据本发明实施例的一种基于高速串行总线的可信平台控制模块的可信系统框图的示意图;

图 6 是根据本发明实施例的一种整机上电时序的示意图;

5 图 7 是根据本发明实施例的一种可信链传递的示意图;

图 8 是根据本发明实施例的一种数据处理装置的示意图;

图 9 是根据本发明实施例的一种计算机终端的结构框图。

具体实施方式

为了使本技术领域的人员更好地理解本发明方案, 下面将结合本发明实施例中的附图, 对本发明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发明一部分的实施例, 而不是全部的实施例。基于本发明中的实施例, 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, 都应当属于本发明保护的范围。

需要说明的是, 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象, 而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换, 以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外, 术语“包括”和“具有”以及他们的任何变形, 意图在于覆盖不排他的包含, 例如, 包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元, 而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

20 首先, 在对本申请实施例进行描述的过程中出现的部分名词或术语适用于如下解释:

可信平台模块 (Trusted Platform Module, 简称为 TPM), 用于在使用设备中集成的专用微控制器处理设备中的加密密钥;

可信平台控制模块 (Trusted Platform Control Module, 简称为 TPCM), 用于建立和保障信任源点, 提供可信平台控制;

25 基本输入输出系统 (Basic Input Output System, 简称为输入输出系统), 是一种业界标准的固件接口;

基板管理控制器 (Baseboard Management Controller, 简称为 BMC), 用于在机器未开机的状态下, 对机器进行固件升级, 查看机器设备等操作;

30 高速串行总线 (Peripheral Component Interface Express, 简称为 PCIE), 用于对点双通道高宽带传输;

可信平台控制模块 (Trusted Platform Control Module, 简称为 TPCM), 是集成在可信计算平台中, 其关键作用在于度量嵌入处理器芯片内的一小块掩模 ROM 或存放启动程序的存储 (Boot Rom), 以及 BMC Boot Rom 等器件, 以避免系统被篡改, 保证服务器安全可信。

5 实施例 1

本发明的实施例可以提供一种数据处理系统, 该数据处理系统可以包括计算机终端, 该计算机终端可以是计算机终端群中的任意一个计算机终端设备。可选地, 在本实施例中, 上述计算机终端也可以替换为移动终端等终端设备。

10 可选地, 在本实施例中, 上述计算机终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

图 1 是根据本发明实施例的一种数据处理系统的流程图。如图 1 所示, 该数据处理系统 100 可以包括: 服务器 102 和智能板卡 104, 服务器 102 与智能板卡 104 通过高速串行总线 PCIE 物理连线连接, 服务器 102 内置串行外设接口总线 SPI。

服务器 102, 用于通过时序控制电路控制智能板卡 104 上电。

15 在该实施例中, 服务器 102 中的时序控制电路控制智能板卡 104 上电, 其中, 服务器 102 可以包括, SPI 开关切换模块, PCIE 开关切换模块, 以及时序控制模块等部分; 时序控制电路可以包括时序控制模块上, 可以用于控制智能板卡 104 和服务器 102 的上电或者解复位时序。

20 可选地, 设备整机上电时, 服务器 102 的时序控制电路通过时序控制模块控制智能板卡 104 上电。

智能板卡 104, 用于在上电且可信的情况下, 将智能板卡 104 的 PCIE 接口模块切换到智能板卡 104 的 SPI 可信度量接口模块, SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器 102 请求待度量的目标数据; 其中, 智能板卡 104 用于获取服务器 102 通过 SPI 发送, 且通过 PCIE 物理连线传输的目标数据, 对目标数据进行可信度量, 得到度量结果; 25 其中, 服务器 102 用于在度量结果表示服务器 102 可信的情况下, 将 SPI 切换至 PCIE, 且通过 PCIE 进行数据传输

在该实施例中, 获取设备整机的上电信号, 基于获取到的上电信号, 服务器 102 的时序控制电路通过时序控制模块控制智能板卡 104 上电, 在上电且可信的情况下, 将智能板卡 104 的 PCIE 接口模块切换至智能板卡 104 的 SPI 可信度量接口模块, 通过 PCIE 物理连 30 线向服务器 102 请求待度量的目标数据, 获取服务器 102 待度量的目标数据, 对获取到的目标数据进行可信度量, 得到度量结果, 其中, 服务器 102 可以用于在度量结果表示服务器 102 可信的情况下, 将 SPI 切换至 PCIE, 且通过 PCIE 物理连线进行数据传输; 目标数

据可以为 BMC FLASH 和 Boot Rom; 度量结果可以为智能板卡 104 完成度量的通知, 可以为可信或不可信的度量结果; PCIE 可以称为高速串行总线。

可选地, 当智能板卡 104 对服务器 102 的目标数据完成度量后, 发出可信信号, 响应智能板卡 104 发出的可信信号, 将 PCIE 切换至串行外设接口总线 SPI, 通过 PCIE 物理连线向智能板卡 104 发送服务器 102 的目标数据, 智能板卡 104 对目标数据进行度量, 得到服务器 102 可信的度量结果。

在本发明实施例中, 服务器 102 和智能板卡 104, 服务器 102 与智能板卡 104 通过高速串行总线 PCIE 物理连线连接, 服务器 102 内置串行外设接口总线 SPI, 其中, 服务器 102, 用于通过时序控制电路控制智能板卡 104 上电; 智能板卡 104, 用于在上电且可信的情况下, 将智能板卡 104 的 PCIE 接口模块切换到智能板卡 104 的 SPI 可信度量接口模块, SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器 102 请求待度量的目标数据; 其中, 智能板卡 104 用于获取服务器 102 通过 SPI 发送, 且通过 PCIE 物理连线传输的目标数据, 对目标数据进行可信度量, 得到度量结果; 其中, 服务器 102 用于在度量结果表示服务器 102 可信的情况下, 将 SPI 切换至 PCIE, 且通过 PCIE 进行数据传输。也就是说, 本发明通过对服务器 102 的 PCIE 物理连线分时复用, 完成服务器 102 启动前的可信度量, 不需要额外增加串行外设接口线缆, 从而达到了提高了对服务器进行可信度量的效率的技术效果, 解决了对服务器进行可信度量的效率低的技术问题。

下面对该实施例的上述方法进行进一步地介绍。

作为一种可选的系统, 服务器包括: SPI 开关切换模块, 用于将 SPI 从切换至 PCIE 物理连线。

在该实施例中, 服务器的时序控制模块收到智能板卡的度量结果, 通过 SPI 开关切换模块将 SPI 总线切换至 PCIE 物理连线, 以从智能板卡切换到服务器的基板管理器 BMC 和中央处理器 CPU。

可选地, 在设备上电后, 服务器可以控制 SPI 开关切换模块, 将 SPI 从切换至 PCIE 物理连线, 此时, 智能板卡可以访问服务器的目标数据, 智能板卡读取服务器的目标数据。

作为一种可选的系统, 服务器包括: 时序控制模块, 用于在智能板卡对目标数据进行可信度量, 得到度量结果之后, 控制 SPI 开关切换模块将 SPI 切换至服务器的基板管理控制器 BMC 和中央处理器 CPU。

在该实施例中, 时序控制模块, 用于在智能板卡对目标数据进行可信度量, 时序控制模块收到智能板卡的度量结果之后, 控制 SPI 开关切换模块将 SPI 从智能板卡切换至基板管理控制器 BMC 和中央处理器 CPU。

可选地, 服务器的时序控制电路通过时序控制模块控制智能板卡上电, 智能板卡完成

自身可信度量后，开始对目标数据进行可信度量，在完成对目标数据的可信度量后，智能板卡控制 SPI 开关切换模块，从 SPI 可信度量接口模块切换到 PCIE 接口模块，控制基板管理控制器 BMC 和中央处理器 CPU，以达到将 SPI 从智能板卡切换至基板管理控制器 BMC 和中央处理器 CPU 的目的。

- 5 可选地，通过 SPI 开关切换模块将 SPI 从智能板卡切换到服务器的基板管理控制器 BMC 和中央处理器 CPU。

作为一种可选的系统，SPI 开关切换模块用于基于 SPI 控制 BMC 访问服务器的第一存储器 BMC Flash 中的数据，且基于 SPI 控制 CPU 访问服务器的第二存储器 Boot Rom 中的数据。

- 10 在该实施例中，SPI 开关切换模块用于控制智能板卡或者服务器 CPU 对 Boot Rom 的访问权限，以及控制智能板卡或者服务器的 BMC 对 BMC Flash 的访问权限。

可选地，在设备上电后，可信度量装置 B 将 SPI 开关（总线）切换到智能板卡，此时智能板卡可以访问服务器的 Boot Rom 和 BMC Flash，智能板卡读取服务器的 Boot Rom 和 BMC Flash 的数据后完成度量。

- 15 作为一种可选的系统，BMC 用于基于服务器的第一存储器 BMC Flash 中的数据进行启动，启动后的 BMC Flash 用于控制 CPU 基于服务器的第二存储器 Boot Rom 中的数据进行启动，启动后的 CPU 控制服务器的操作系统启动，以控制 PCIE 进行数据传输。

- 20 在该实施例中，对基板管理控制器 BMC 和中央处理器 CPU 进行上电或解复位，以使上电或解复位后的基板管理控制器 BMC 和中央处理器 CPU 读取存储器中的目标数据完成启动，基板管理控制器 BMC 和中央处理器 CPU 加载输入输出系统程序，用于初始化系统硬件，同时，引导服务器的系统启动，其中，服务器的系统启动可以为服务器的操作系统（Operation System，简称为 OS）；PCIE，启动后的 CPU 控制服务器的操作系统启动，以控制 PCIE 进行数据传输。

- 25 可选地，基板管理控制器 BMC 和中央处理器 CPU 上电或者解复位，读取基板管理控制器中的第一存储器 BMC Flash 完成启动，启动后的 BMC Flash 用于控制 CPU 上电或者解复位，CPU 读取服务器的第二存储器 Boot Rom 中的数据完成启动，启动后 CPU 控制所述服务器的操作系统启动，以达到控制所述 PCIE 进行数据传输的目的。

- 30 可选地，Boot Rom 存储着输入输出程序（BIOS 程序）或统一的可扩展固件接口（Unified Extensible Firmware Interface，简称为 UEFI）的输入输出系统程序（UEFI BIOS 程序），中央处理器启动时首先从 BMC Flash 中加载输入输出系统程序，用于初始化系统硬件，然后引导服务器的系统启动，达到使得服务器的系统在可信的环境启动运行的目的。

作为一种可选的系统，目标数据包括 BMC Flash 中的数据和 Boot Rom 中的数据。

在该实施例中，智能板卡对目标数据进行度量，即智能板卡对服务器的 Boot Rom 和 BMC Flash 中的数据进行度量。

可选地，BMC Flash 中存储着 BMC 程序，用于确保智能板卡 CPU 中操作系统的可信；Boot Rom 中存储着 BIOS 程序或 UEFI BIOS 程序，用于初始化系统硬件，引导操作系统启动。

作为一种可选的系统，服务器包括：PCIE 开关切换模块，用于将 SPI 切换至 PCIE。

在该实施例中，PCIE 开关切换模块用于将 PCIE 插槽物理连线切换到 SPI 和时序控制模块，或者将 SPI 切换到 CPU 的 PCIE 总线上，以实现了 PCIE 插槽物理线路的分时复用。

可选地，通过 PCIE 开关切换模块，将 PCIE 总线从智能板卡切换到服务器的基板管理控制器和中央处理器；通过 PCIE 开关切换模块利用 PCIE 物理连线，以将从 SPI 切换至 PCIE。

作为一种可选的系统，智能板卡包括：接口切换模块，用于 PCIE 接口模块切换到 SPI 可信度量接口模块。

在该实施例中，智能板卡包括：接口切换模块，利用接口切换模块，达到将 PCIE 接口模块切换到 SPI 可信度量接口模块的目的。

在该实施例中，智能板卡包括：SPI 可信度量接口模块，其中，SPI 可信度量接口模块用于实现 SPI 总线功能，通过 SPI 访问服务器的 Boot Rom 和 BMC Flash 等器件，以达到获取目标数据的目的。

可选地，当智能板卡对服务器的目标数据完成度量后，发出可信信号，响应智能板卡发出的可信信号，通过串行外设接口总线向智能板卡发送服务器的目标数据。

作为一种可选的系统，接口切换模块还用于在对目标数据进行可信度量，得到度量结果之后，将 SPI 可信度量接口模块切换至 PCIE 接口模块。

在该实施例中，智能板卡包括：接口切换模块，用于在对目标数据进行可信度量，得到度量结果之后，将 SPI 可信度量接口模块切换至智能板卡的 PCIE 接口模块，利用 PCIE 接口模块使得智能板卡进入 PCIE 接口模式。

可选地，接口切换模块用于切换 SPI 可信度量接口模块和 PCIE 接口模块，在设备上电后，工作在 SPI 可信度量接口模式下进行度量，在完成度量后，接口切换模块将 SPI 可信度量接口模块切换至智能板卡的 PCIE 接口模块。

作为一种可选的系统，智能板卡包括：可信平台控制模块 TPCM，用于对智能板卡的操作系统进行可信度量，其中，可信的操作系统用于对目标数据进行可信度量，得到度量结果。

在该实施例中，智能板卡包括：可信平台控制模块 TPCM，利用可信的操作系统用于对目标数据进行可信度量，得到度量结果。

可选地，TPCM 模块，用于度量智能板卡的 Boot Rom 和 BMC Flash，Boot Rom 确保智能板卡 CPU 运行 OS 的可信。智能板卡 CPU 启动 OS 后，运行 swtpm (software TPM) 程序用于对服务器完成度量。

在本发明实施例中，数据处理系统可以包括服务器和智能板卡，服务器和智能板卡，服务器与智能板卡通过高速串行总线 PCIE 物理连线连接，服务器内置串行外设接口总线 SPI，其中，服务器，用于在上电且可信的情况下，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据；其中，智能板卡用于获取服务器通过 SPI 发送，且通过 PCIE 物理连线传输的目标数据，对目标数据进行可信度量，得到度量结果；其中，服务器用于在度量结果表示服务器可信的情况下，将 SPI 切换至 PCIE，且通过 PCIE 进行数据传输。也就是说，本发明通过对服务器的 PCIE 物理连线分时复用，完成服务器启动前的可信度量，不需要额外增加串行外设接口线缆，从而达到了提高对服务器进行可信度量的效率的技术效果，解决了对服务器进行可信度量的效率低的技术问题。

实施例 2

根据本发明实施例，还提供了一种数据处理方法的实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

本申请实施例一所提供的方法实施例可以在移动终端、计算机终端或者类似的运算装置中执行。图 2 示出了一种用于实现数据处理方法的计算机终端（或移动设备）的硬件结构框图。如图 2 所示，计算机终端 20（或移动设备 20）可以包括一个或多个（图中采用 202a、202b，……，202n 来示出）处理器 202（处理器 202 可以包括但不限于微处理器 MCU 或可编程逻辑器件 FPGA 等的处理装置）、用于存储数据的存储器 204、以及用于通信功能的传输装置 206。除此以外，还可以包括：显示器、输入/输出接口（I/O 接口）、通用串行总线（USB）端口（可以作为 I/O 接口的端口中的一个端口被包括）、网络接口、电源和/或相机。本领域普通技术人员可以理解，图 2 所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，计算机终端 20 还可包括比图 2 中所示更多或者更少的组件，或者具有与图 2 所示不同的配置。

应当注意到的是上述一个或多个处理器 202 和/或其他数据处理电路在本文中通常可以被称为“数据处理电路”。该数据处理电路可以全部或部分的体现为软件、硬件、固件或其他任意组合。此外，数据处理电路可为单个独立的处理模块，或全部或部分的结合到计

算机终端 20(或移动设备)中的其他元件中的任意一个内。如本申请实施例中所涉及到的,该数据处理电路作为一种处理器控制(例如与接口连接的可变电阻终端路径的选择)。

存储器 204 可用于存储应用程序的软件程序以及模块,如本发明实施例中的数据处理方法对应的程序指令/数据存储装置,处理器 202 通过运行存储在存储器 204 内的软件程序以及模块,从而执行各种功能应用以及数据处理,即实现上述的应用程序的数据处理方法。5 存储器 204 可包括高速随机存储器,还可包括非易失性存储器,如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中,存储器 204 可进一步包括相对于处理器 202 远程设置的存储器,这些远程存储器可以通过网络连接至计算机终端 20。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

10 传输装置 206 用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端 20 的通信供应商提供的无线网络。在一个实例中,传输装置 206 包括一个网络适配器(Network Interface Controller, NIC),其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中,传输装置 206 可以为射频(Radio Frequency, RF)模块,其用于通过无线方式与互联网进行通讯。

15 显示器可以例如触摸屏式的液晶显示器(LCD),该液晶显示器可使得用户能够与计算机终端 20(或移动设备)的用户界面进行交互。

此处需要说明的是,在一些可选实施例中,上述图 2 所示的计算机设备(或移动设备)可以包括硬件元件(包括电路)、软件元件(包括存储在计算机可读介质上的计算机代码)、或硬件元件和软件元件两者的结合。应当指出的是,图 2 仅为特定具体实例的一个实例,20 并且旨在示出可存在于上述计算机设备(或移动设备)中的部件的类型。

在图 2 所示的运行环境下,本申请提供了如图 3 所示的数据处理方法。需要说明的是,该实施例的数据处理方法可以由图 2 所示实施例的移动终端执行。

图 3 是根据本发明实施例的一种数据处理方法的流程图。如图 3 所示,该方法可以包括以下步骤。

25 步骤 S302,响应于智能板卡上电且可信,将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块,其中,SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据。

在本发明上述步骤 S302 提供的技术方案中,获取设备上电信号,基于获取到的上电信号,高速串行总线 PCIE 切换至串行外设接口总线 SPI,以服务器切换至智能板卡,以使30 服务器与智能板卡相连接,对智能板卡进行度量,发出可信的度量结果,响应于智能板卡可信的度量结果,通过串行外设接口总线 SPI 向智能板卡发送服务器待度量的目标数据。

可选地,当智能板卡对服务器的存放启动程序的存储和基板管理控制器的闪存的数据

后完成度量后，发出可信信号，响应智能板卡发出的可信信号，通过串行外设接口总线向智能板卡发送服务器待度量的目标数据。

步骤 S304，获取服务器通过内置的串行外设接口总线 SPI 发送，且通过 PCIE 物理连线传输的目标数据。

5 在本发明上述步骤 S304 提供的技术方案中，基于上电信号控制串行外设接口总线 SPI，以将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，通过 PCIE 物理连线传输的目标数据。

 可选地，在设备上电后，基于上电信号控制串行外设接口总线 SPI，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，此时通过 PCIE 物理连线传输的目标
10 数据，以实现将目标数据从服务器的存储器发送至目标板卡的目的。

 步骤 S306，对目标数据进行可信度量，得到度量结果，其中，在度量结果表示服务器可信时，SPI 由服务器切换至 PCIE，且服务器通过 PCIE 进行数据传输。

 在本发明上述步骤 S306 提供的技术方案中，对目标数据进行可信度量，得到度量结果，当度量结果表示服务器可信时，SPI 由服务器切换至 PCIE，且服务器通过 PCIE 进行
15 数据传输。

 在本发明实施例中，响应于智能板卡上电且可信，将服务器与智能板卡之间的高速串行总线 PCIE 切换至串行外设接口总线 SPI，且通过 SPI 获取服务器待度量的目标数据，且对目标数据进行可信度量，得到度量结果；响应于度量结果表示服务器可信，则将 SPI 切换至 PCIE，且通过 PCIE 进行数据传输。也就是说，本发明通过对服务器的 PCIE 物理连
20 线分时复用，完成服务器启动前的可信度量，不需要额外增加串行外设接口线缆，从而达到了提高对服务器进行可信度量的效率的技术效果，解决了对服务器进行可信度量的效率低的技术问题。

实施例 3

 下面对该实施例的上述方法的优选实施方式进行进一步介绍，具体以一种基于高速串行总线的可信校验进行说明。
25

 目前，对服务器进行可信度量，一是外接串行外设接口 (Serial Peripheral Interface，简称为串行外设接口) 总线，该方法虽然可以是节省可信平台控制模块芯片成本，实现了单一可信链传递，但对信号质量挑战很大且不稳定；二是外接串行外设接口线缆的方案，但是该方法极大限制了系统的可扩展性；三是外接串行外设接口总线，但是该方法增加了 IO
30 接口的资源消耗。

 为解决上述问题，相关技术可以是将智能板卡与服务器上的 TPCM 可信模块都作为度量各自系统可信的模块，图 4 是根据本发明相关技术中的一种存在两个可信平台控制模块

可信模块的服务器的示意图，如图 4 所示，服务器包括中央处理器、基板管理控制器、Boot Rom、BMC FLASH、时序控制电路、以及可信平台控制模块等部分，其中，Boot Rom 中存储着输入输出系统或统一的可扩展固件接口（Unified Extensible Firmware Interface，简称为 UEFI）的输入输出系统程序，中央处理器启动时首先从 Boot Rom 加载 BIOS 程序，用于初始化系统硬件，并引导操作系统启动；BMC FLASH 存储着 BMC 程序，BMC 启动时首先加载 BMC 程序；可信平台控制模块可信模块，在服务器上电后最先启动。在中央处理器和 BMC 启动前，度量 Boot Rom 数据和 BMC FLASH 数据，确保 Boot Rom 数据和 BMC FLASH 数据可信。之后可信平台控制模块通知时序控制电路，控制中央处理器和基板管理控制器上电或者解复位，使得服务器在可信的环境启动运行。

- 10 服务器上存在高速串行总线插槽，高速串行总线插槽可以插入智能板卡；智能板卡上包括中央处理器，基板管理控制器，以及可信平台控制模块等部分；智能板卡上可信平台控制模块可信度量过程与服务器上基本一致。

- 但是，上述方法中的服务器和智能板卡都存在可信平台控制模块可信模块，增加了物料成本以及后期运维成本；服务器可信由服务器上的可信平台控制模块可信模块度量，二者强绑定，在云计算使用场景无法支持迁移；服务器和智能板卡都存在可信平台控制模块可信模块，使得整个系统中存在两条可信链，一条是服务器上可信平台控制模块到 Boot Rom 中数据和 BMC FLASH 数据到系统的可信链，另一条是智能板卡上可信平台控制模块到 Boot Rom 中数据和 BMC FLASH 数据到系统的可信链。

- 在另一种相关技术中，将服务器上的可信平台控制模块可信模块去掉，只保留智能板卡上的可信平台控制模块可信模块，但是该方法中智能网卡与服务器之间通过高速串行总线连接，可信平台控制模块可信模块无法在服务器的中央处理器启动前完成对服务器的 Boot Rom 中数据和 BMC FLASH 数据的度量，因而额外引入了串行外设接口线号，用于通知服务器时序控制电路对中央处理器和基板管理控制器的上电或者解复位的控制线，串行外设接口线缆实现服务器的 Boot Rom 中数据和 BMC FLASH 数据的访问，因而可以度量 Boot Rom 中数据和 BMC FLASH 数据，同时串行外设接口线缆中包含控制信号。

- 上述方法额外串行外设接口线缆存在信号质量问题，硬件链路上不可靠；额外串行外设接口链路增加了智能网卡上接口的使用量，增加资源消耗，在单个智能板卡接入多个服务器的情况下，额外的串行外设接口资源消耗可能导致规格下降；单个智能板卡接入多个服务器的情况下，需要增加多条额外串行外设接口线缆，安装维护复杂。

- 30 为解决上述问题，该实施例提出了此提出基于高速串行总线的可信度量，实现了不需要外接串行外设接口线缆即可实现系统对服务器可信度量，既保留了外接串行外设接口方案的优势，也解决了其劣势。

图 5 是根据本发明实施例的一种数据处理方法的示意图，如图 5 所示，服务器包括：

中央处理器、基板管理控制器 BMC、Boot Rom、BMC FLASH、时序控制电路(模块)、可信平台控制模块可信模块以及可信度量装置 B 等部分, 其中, 服务器上可信装置 B 包括: SPI 开关切换模块, 高速串行总线开关切换模块, 以及时序控制模块等部分; 智能板卡包括: 中央处理器, 基板管理控制器 BMC, Boot Rom, BMC FLASH, 可信平台控制模块可信模块以及可信度量装置 A 等部分, 其中, 智能板卡上可信装置 A 包括: 串行外设接口可信度量接口模块, 高速串行总线接口模块, 以及接口切换模块等部分。智能板卡通过高速串行总线插槽与服务器相连。

可选地, 智能板卡上 Boot Rom, 存储着输入输出系统或统一可扩展接口固件的输入输出系统程序, 中央处理器启动时首先从 Boot Rom 中加载输入输出系统程序, 用于初始化系统硬件, 并引导操作系统启动; BMC FLASH, 存储着 BMC 程序, 基板管理控制器启动时首先加载基板管理控制器程序。

可选地, 可信平台控制模块, 用于度量智能板卡的 Boot Rom 中数据和 BMC FLASH 数据, Boot Rom 确保智能板卡中央处理器运行操作系统的可信。智能板卡中央处理器启动操作系统后, 运行可信平台模块软件 (software TPM, 简称为 swtpm) 的程序对服务器完成度量。

可选地, 串行外设 SPI 接口可信度量接口模块, 实现了 SPI 总线功能, 用于访问服务器的 Boot Rom 和 BMC FLASH 等器件。高速串行总线 PCIE 接口模块用于实现高速串行总线设备, 在智能板卡完成对服务器的 Boot Rom 和 BMC FLASH 中的数据的度量后, 接口工作在高速串行总线接口模式。

可选地, 接口切换模块, 用于切换串行外设接口可信度量接口模块和高速串行总线接口模块, 在设备上电后, 可信度量装置 A 工作在串行外设接口可信度量接口模式下, 完成度量后, 中央处理器通过接口切换模块将可信装置 A 切换为高速串行总线接口模式。

可选地, 服务器上可信装置 B 中的 SPI 开关切换模块, 用于控制智能板卡或者服务器中央处理器对 Boot Rom 的访问权限, 以及控制智能板卡或者服务器基板管理控制器对 BMC FLASH 的访问权限。在设备上电后, 可信度量装置 B 将 SPI 开关切换模块切换到智能板卡, 此时智能板卡可以访问服务器的 Boot Rom 和 BMC FLASH, 智能板卡读取服务器的 Boot Rom 和 BMC FLASH 的数据后完成度量。

当智能板卡对服务器的 Boot Rom 和 BMC FLASH 的数据后完成度量后, 可信装置 B 将 BMC FLASH 开关切换到服务器的基板管理控制器, 此时服务器基板管理控制器可以访问 BMC FLASH, 将 Boot Rom SPI 开关切换模块切换到服务器的中央处理器, 此时服务器中央处理器可以访问 Boot Rom。高速串行总线开关切换模块用于将高速串行总线插槽物理连线切换到串行外设接口和时序控制模块, 或者切换到中央处理器的高速串行总线上, 实现了高速串行总线插槽物理线路的分时复用。

可选地，服务器上可信装置 B 中的时序控制模块，用于控制智能板卡，服务器的上电或者解复位时序，当设备上电时，服务器时序控制电路通过时序控制模块控制智能板卡上电，智能板卡完成自身可信度量后，开始度量服务器的 Boot Rom 和 BMC FLASH，在完成对服务器的 Boot Rom 和 BMC FLASH 的数据的度量后，智能板卡将可信度量装置 A 的接口从串行外设接口可信度量接口模块切换到高速串行总线接口模块，并通知服务器的可信度量装置 B 的时序控制模块。时序控制模块收到智能板卡完成度量的通知，通过 SPI 开关切换模块将串行外设接口总线从智能板卡切换到服务器的基板管理控制器和中央处理器；通过高速串行总线开关切换模块将高速串行总线插槽物理连线从串行外设接口总线切换到高速串行总线，之后对基板管理控制器上电或者解复位，基板管理控制器读取 BMC FLASH 数据完成启动，再对中央处理器上电或者解复位，中央处理器读取 Boot Rom 完成启动，中央处理器启动后输入输出系统或者 UEFI 输入输出系统可以正常扫描智能板卡的高速串行总线，服务器 OS 启动后的可信度量通过高速串行总线完成数据传输。

需要说明的是，服务器高速串行总线首先需要经过中央处理器枚举配置后才能使用，而中央处理器枚举配置高速串行总线依赖 Boot Rom 中输入输出系统程序的执行，输入输出系统程序的执行又依赖可信平台控制模块可信度量，为了解决此问题，本发明将 PCIE 物理连线复用为串行外设接口总线，以及时序控制信号线，以保证智能板卡先对服务器的 Boot Rom 和 BMC FLASH 完成度量之后，再启动服务器扫描高速串行总线。

图 6 是根据本发明实施例的一种整机上电时序的示意图，如图 6 所示，本发明的整机上电时序步骤如下。

步骤 S601，电源上电。

在该实施例中，可以是整机设备的电源上电。

步骤 S602，智能板卡的 TPCM 上电。

在该实施例中，服务器的时序控制电路控制智能板卡的 TPCM 上电。

步骤 S603，智能板卡的 TPCM 完成智能板卡的 Boot Rom 和 BMC Flash 可信度量。

在该实施例中，智能板卡的 TPCM 完成智能板卡的 Boot Rom 和 BMC Flash 可信度量，智能板卡的 BMC 和 CPU 上电。

步骤 S604，智能板卡的 TPCM 对操作系统的可信度量可度量。

在该实施例中，智能板卡的 TPCM 完成智能板卡的 Boot Rom 和 BMC Flash 可信度量，智能板卡的 BMC 和 CPU 上电，智能板卡可信平台控制模块完成智能板卡对操作系统的可信度量。

步骤 S605，OS 启动完成运行 swtpm。

在该实施例中，操作系统启动完成运行可信平台模块软件，智能板卡可信平台控制模块完成智能板卡对操作系统的可信度量，反馈可信的度量结果，操作系统启动完成运行可信平台模块软件。

步骤 S606，对服务器的 Boot Rom 和 BMC Flash 可信度量。

- 5 在该实施例中，操作系统启动完成运行可信平台模块软件，智能板卡操作系统完成对服务器的 Boot Rom 和 BMC Flash 的可信度量。

步骤 S607，SPI 总线和 PCIE 总线开关切换。

在该实施例中，智能板卡操作系统完成对服务器的 Boot Rom 和 BMC Flash 的可信度量之后，通知服务器时序控制模块，完成串行外设接口 SPI 总线和高速串行 PCIE 总线开关切换。

10

步骤 S608，服务器的 BMC 和中央处理器上电。

在该实施例中，串行外设接口总线和高速串行总线开关切换，通过服务器时序控制电路将服务器的 BMC 和中央处理器上电。

步骤 S609，整机上电完成。

- 15 图 7 是根据本发明实施例的一种可信链传递的示意图，如图 7 所示，该系统可信链的传递过程可以包括以下步骤。

步骤 S701，服务器操作系统。

在该实施例中，启动服务器操作系统。

步骤 S702，服务器的 Boot Rom。

- 20 在该实施例中，智能板卡的 Boot Rom 程序启动，度量智能板卡操作系统 OS，以保证智能板卡 OS 可信。

步骤 S703，智能板卡 OS。

在该实施例中，智能板卡的 Boot Rom 程序启动，度量智能板卡操作系统，保证智能板卡操作系统（Operating System，简称为 OS）可信。

25

步骤 S704，智能板卡的 Boot Rom。

在该实施例中，智能板卡操作系统程序启动，度量服务器的 Boot Rom，保证服务器的 Boot Rom 可信。

步骤 S705，智能板卡的 TCMP。

在该实施例中，服务器的 Boot Rom 程序启动，度量服务器操作系统，保证服务器操作系统可信。

30

本发明通过对服务器 PCIE 物理连线的分时复用，完成服务器启动前的可信度量，通过可信度量装置完成总线切换及时序控制，从而达到了一下几点技术效果：不需要额外增加串行外设接口线缆，智能板卡只需插入高速串行总线插槽即可完成对服务器的可信度量；智能板卡可信平台控制模块是整个系统唯一可信根，单一可信链从智能板卡传递到服务器；

5 智能板卡操作系统运行可信平台模块软件对服务器可信度量，灵活度高，可热升级，可迁移；整机只需一个可信平台控制模块完成可信链串联，降低物料成本和运维成本；节省智能板卡接口资源；单个智能板卡连接多个服务器的场景也可以支持可信度量。

需要说明的是，对于前述的各方法实施例，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，本发明并不受所描述的动作顺序的限制，因为

10 依据本发明，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，所涉及的动作和模块并不一定是本发明所必须的。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的资源配置方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但

15 很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献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（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

实施例 4

20 根据本发明实施例，还提供了一种用于实施上述图 3 所示的数据处理方法的数据处理装置。

图 8 是根据本发明实施例的一种数据处理装置的示意图。如图 8 所示，该数据处理装置 800 可以包括：第一切换单元 802、第一获取单元 804 和第二切换单元 806。

第一切换单元 802，用于响应于智能板卡上电且可信，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，其中，SPI 可信度量接口模块用于通过 PCIE 物理

25 连线向服务器请求待度量的目标数据。

第一获取单元 804，用于获取服务器通过内置的串行外设接口总线 SPI 发送，且通过 PCIE 物理连线传输的目标数据

第二切换单元 806，用于对目标数据进行可信度量，得到度量结果，其中，在度量结果

30 表示服务器可信时，SPI 由服务器切换至 PCIE，且服务器通过 PCIE 进行数据传输。

此处需要说明的是，上述第一切换单元 802、第一获取单元 804 和第二切换单元 806 对应于实施例 2 中的步骤 S302 至步骤 S306，三个单元与对应的步骤所实现的实例和应用

场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述单元作为装置的一部分可以运行在实施例一提供的计算机终端 A 中。

在该实施例的资源配置装置中，通过第一切换单元，响应于智能板卡上电且可信，将服务器与智能板卡之间的高速串行总线 PCIE 切换至串行外设接口总线 SPI，且通过 SPI 获取服务器待度量的目标数据，且对目标数据进行可信度量，得到度量结果；通过第二切换单元，响应于度量结果表示服务器可信，则将 SPI 切换至 PCIE，且通过 PCIE 进行数据传输。也就是说，本发明通过对服务器的第一目标总线分时复用，完成服务器启动前的可信度量，不需要额外增加串行外设接口线缆，从而达到了提高对服务器进行可信度量的效率的技术效果，解决了对服务器进行可信度量的效率低的技术问题。

10 实施例 5

图 9 是根据本发明实施例的一种计算机终端的结构框图。如图 9 所示，该计算机终端 A 可以包括：一个或多个（图中仅示出一个）处理器 902、存储器 904、以及传输装置 906。

其中，存储器可用于存储软件程序以及模块，如本发明实施例中的数据处理方法和装置对应的程序指令/模块，处理器通过运行存储在存储器内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的数据处理方法。存储器可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器可进一步包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至终端 A。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

处理器可以通过传输装置调用存储器存储的信息及应用程序，以执行下述步骤：响应于智能板卡上电且可信，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，其中，SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据；获取服务器通过内置的串行外设接口总线 SPI 发送，且通过 PCIE 物理连线传输的目标数据；对目标数据进行可信度量，得到度量结果，其中，在度量结果表示服务器可信时，SPI 由服务器切换至 PCIE，且服务器通过 PCIE 进行数据传输。

本发明实施例，提供了一种数据处理方法，通过对服务器的 PCIE 物理连线分时复用，完成服务器启动前的可信度量，不需要额外增加串行外设接口线缆，从而达到了提高对服务器进行可信度量的效率的技术效果，解决了对服务器进行可信度量的效率低的技术问题。

本领域普通技术人员可以理解，图 9 所示的结构仅为示意，计算机终端 A 也可以是智能手机（如 Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices, MID）、PAD 等终端设备。图 9 并不对上述计算机终端 A 的结构造成限定。例如，计算机终端 A 还可包括比图 9 所示更多或者更少的组件（如网络接口、显示装置等），或者具有与图 9 所示不同的配置。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器(Read-Only Memory, ROM)、随机存取器(Random Access Memory, RAM)、磁盘或光盘等。

5 实施例 6

本发明的实施例还提供了一种计算机可读存储介质。可选地，在本实施例中，上述计算机可读存储介质可以用于保存上述实施例一所提供的数据处理方法所执行的程序代码。

作为一种可选的示例，计算机可读存储介质被设置为存储用于执行以下步骤的程序代码：响应于智能板卡上电且可信，将智能板卡的 PCIE 接口模块切换到智能板卡的 SPI 可信度量接口模块，其中，SPI 可信度量接口模块用于通过 PCIE 物理连线向服务器请求待度量的目标数据；获取服务器通过内置的串行外设接口总线 SPI 发送，且通过 PCIE 物理连线传输的目标数据；对目标数据进行可信度量，得到度量结果，其中，在度量结果表示服务器可信时，SPI 由服务器切换至 PCIE，且服务器通过 PCIE 进行数据传输。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

在本申请所提供的几个实施例中，应该理解到，所揭露的技术内容，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元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存储介质中。基于这样的理解，本发明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全部或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计算机设备

(可为个人计算机、服务器或者网络设备等)执行本发明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、只读存储器 (ROM, Read-Only Memory)、随机存取存储器 (RAM, Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

- 5 以上所述仅是本发明的优选实施方式, 应当指出, 对于本技术领域的普通技术人员来说, 在不脱离本发明原理的前提下, 还可以做出若干改进和润饰, 这些改进和润饰也应视为本发明的保护范围。

权 利 要 求 书

1. 一种数据处理系统，其特征在于，包括：服务器和智能板卡，所述服务器与所述智能板卡通过高速串行总线 PCIE 物理连线连接，所述服务器内置串行外设接口总线 SPI，其中，
- 5 所述服务器，用于通过时序控制电路控制所述智能板卡上电；
 所述智能板卡，用于在上电且可信的情况下，将所述智能板卡的 PCIE 接口模块切换到所述智能板卡的 SPI 可信度量接口模块，所述 SPI 可信度量接口模块用于通过所述 PCIE 物理连线向所述服务器请求待度量的目标数据；
 其中，所述智能板卡用于获取所述服务器通过所述 SPI 发送，且通过所述 PCIE 物理连线传输的所述目标数据，对所述目标数据进行可信度量，得到度量结果；
- 10 其中，所述服务器用于在所述度量结果表示所述服务器可信的情况下，将所述 SPI 切换至所述 PCIE，且通过所述 PCIE 进行数据传输。
2. 根据权利要求 1 所述的系统，其特征在于，所述服务器包括：SPI 开关切换模块，用于将所述 SPI 切换至所述 PCIE 物理连线。
- 15 3. 根据权利要求 2 所述的系统，其特征在于，所述服务器包括：
 时序控制模块，用于在所述智能板卡对所述目标数据进行可信度量，得到所述度量结果之后，控制所述 SPI 开关切换模块将所述 SPI 切换至所述服务器的基板管理控制器 BMC 和中央处理器 CPU。
- 20 4. 根据权利要求 3 所述的系统，其特征在于，所述 SPI 开关切换模块用于基于所述 SPI 控制所述 BMC 访问所述服务器的第一存储器 BMC Flash 中的数据，且基于所述 SPI 控制所述 CPU 访问所述服务器的第二存储器 Boot Rom 中的数据。
- 25 5. 根据权利要求 4 所述的系统，其特征在于，所述 BMC 用于基于所述 BMC Flash 中的数据进行启动，启动后的所述 BMC Flash 用于控制所述 CPU 基于所述 Boot Rom 中的数据进行启动，启动后的所述 CPU 用于控制所述服务器的操作系统启动，以控制所述 PCIE 进行数据传输。
6. 根据权利要求 4 所述的系统，其特征在于，所述目标数据包括所述 BMC Flash 中的数据和所述 Boot Rom 中的数据。
7. 根据权利要求 1 所述的系统，其特征在于，所述服务器包括：
 PCIE 开关切换模块，用于将所述 SPI 切换至所述 PCIE。
- 30 8. 根据权利要求 1 所述的系统，其特征在于，所述智能板卡包括：

接口切换模块，用于所述 PCIE 接口模块切换到所述 SPI 可信度量接口模块。

9. 根据权利要求 8 所述的系统，其特征在于，所述接口切换模块还用于在对所述目标数据进行可信度量，得到所述度量结果之后，将所述 SPI 可信度量接口模块切换至所述 PCIE 接口模块。
- 5 10. 根据权利要求 1 至 9 中任意一项所述的系统，其特征在于，所述智能板卡包括：
- 可信平台控制模块 TPCM，用于对所述智能板卡的操作系统进行可信度量，其中，可信的所述操作系统用于对所述目标数据进行可信度量，得到所述度量结果。
11. 一种数据处理方法，其特征在于，包括：
- 10 响应于智能板卡上电且可信，将所述智能板卡的 PCIE 接口模块切换到所述智能板卡的 SPI 可信度量接口模块，其中，所述 SPI 可信度量接口模块用于通过所述 PCIE 物理连线向服务器请求待度量的目标数据；
- 获取所述服务器通过内置的串行外设接口总线 SPI 发送，且通过所述 PCIE 物理连线传输的所述目标数据；
- 15 对所述目标数据进行可信度量，得到度量结果，其中，在所述度量结果表示所述服务器可信时，所述 SPI 由所述服务器切换至所述 PCIE，且所述服务器通过所述 PCIE 进行数据传输。
12. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质包括存储的程序，其中，在所述程序被处理器运行时控制所述计算机可读存储介质所在设备执行权利要求 11 所述的方法。