(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 8 月 31 日 (31.08.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/143757 A1

(51) 国际专利分类号:
G06F 21/57 (2013.01)

(21) 国际申请号: PCT/CN2016/097668

(22) 国际申请日: 2016 年 8 月 31 日 (31.08.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610109021.6 2016 年 2 月 26 日 (26.02.2016) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 叶思海 (YE, Sihai); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 施迅 (SHI, Xun); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (LONGSUN LEAD IP LTD.); 中国北京市海淀区北清路 68 号院 3 号楼 101, Beijing 100094 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) Title: TRUSTWORTHINESS MEASURING METHOD AND DEVICE FOR CLOUD COMPUTING PLATFORM

(54) 发明名称 : 云计算平台的可信度量方法和装置

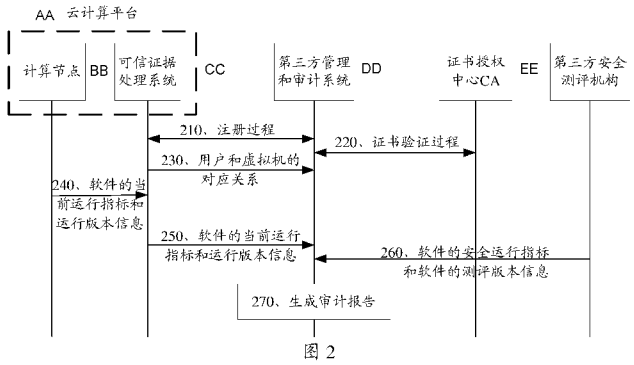

图 2

210	REGISTRATION PROCESS
220	CERTIFICATE VERIFICATION PROCESS
230	CORRELATION BETWEEN A USER AND A VIRTUAL MACHINE
240	CURRENT OPERATION INDEX AND OPERATION VERSION INFORMATION OF SOFTWARE
250	CURRENT OPERATION INDEX AND OPERATION VERSION INFORMATION OF THE SOFTWARE
260	OPERATION SECURITY INDEX OF THE SOFTWARE AND ASSESSMENT VERSION INFORMATION OF THE SOFTWARE
270	GENERATE AN AUDIT REPORT
AA	CLOUD COMPUTING PLATFORM
BB	COMPUTING NODE
CC	TRUSTWORTHINESS EVIDENCE PROCESSING SYSTEM
DD	THIRD-PARTY MANAGING AND AUDITING SYSTEM
EE	CERTIFICATE AUTHORITY CA
FF	THIRD-PARTY SECURITY ASSESSMENT ORGANIZATION

(57) Abstract: A trustworthiness measuring method for a cloud computing platform, the method comprising: a third-party managing and auditing system receiving the current operation index of software in a cloud computing platform, the current operation index of the software being signed using a Digital Certificate issued by the Certificate Authority via a trusted platform of the could computing platform; the third-party managing and auditing system acquiring an operation security index of the software from a third party assessment organization; and the third-party managing and auditing system generating an audit report according to the current operation index of the software signed by the Digital Certificate and the operation security index of the software, the audit report being used for indicating the degree of trustworthiness of the cloud computing platform. The invention makes the trustworthiness measuring process of the cloud computing platform open and transparent, improving the authenticity of trustworthiness measurement of the cloud computing platform, thereby improving the user's trust in the cloud computing platform.

(57) 摘要: 一种云计算平台的可信度量方法，该方法包括：第三方管理和审计系统接收云计算平台中的软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心颁布的数字证书进行签名；所述第三方管理和审计系统从第三方测评机构获取所述软件的安全运行指标；所述第三方管理和审计系统根据经过所述数字证书签名的所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。使得云计算平台的可信度量过程公开，透明，提高了云计算平台的可信度量的真实性，从而提高用户对该云计算平台的信任。

WO 2017/143757 A1

云计算平台的可信度量方法和装置

本申请要求于 2016 年 2 月 26 日提交中国专利局、申请号为 201610109021.6、发明名称为“云计算平台的可信度量方法和装置”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，尤其涉及云计算平台的可信度量方法和装置。

背景技术

云计算平台可以允许用户通过无所不在的、便捷的、按需获得的网络接入到一个可动态配置的共享计算资源池，该共享计算资源池包括网络设备、服务器、存储设备、应用以及业务。云计算平台可以以较小的管理代价，或者用户与业务提供者较低的交互复杂度，实现上述可配置计算资源的快速发放与发布。

用户把数据迁移到云计算平台后，对数据的所有权和控制权分离，用户是数据的所有者，但对数据的控制权却交给云计算平台的提供商，所有与数据相关的计算、存储等资源类操作都是用户通过云计算平台完成的。这样，云计算平台要获得真正大规模的发展和应用，首先要解决云计算平台中的安全问题。

图 1 示出了现有技术中对云计算平台进行可信度量的架构的示意图。在图 1 所示的架构中，用户可以通过对验证服务器的直接信任，以及验证服务器对云计算平台的信任，建立对云计算平台的间接信任。在验证服务器与云计算平台建立信任的过程中，验证服务器可以通过云计算节点中布置的可信赖平台模块（Trusted Platform Module，TPM）安全芯片、中央处理器（Central Processing Unit，CPU）/基本输入输出系统（Basic Input Output System，BIOS）的硬件能力以及可信赖计算组织（Trusted Computing Group，TCG）的规范，在技术上信任云计算平台，也就是说，云计算平台可以在技术上保证向验证服务器发送的软件的当前运行指标是真实的。

然而，图 1 所示的架构中，由于验证服务器和云计算平台都属于云计算平台的提供商管控，云计算平台的可信度量过程都可以由内部远程证明和审

计系统实现，而这一内部远程证明和审计过程对用户来说是不透明的，并且没有可信第三方机构的监管，上述过程中会存在各种未知的风险，使得云计算平台的可信度降低。例如，在上述过程中，可信平台的数字证书和云计算平台的数字证书可以是由提供商颁布的内部数字证书，当提供商需要在验证内部数字证书时，再将该内部数字证书转换成符合证书授权中心（Certification Authority，CA）标准的数字证书进行验证，提供商可能会替换内部数字证书，从而无法保证内部数字证书对应的数字签名的真实性，同时，经过该数字签名的度量信息的真实性也无法保证，存在度量信息被篡改的可能。

发明内容

本申请的目的是提供一种改进的云计算平台的可信度量的方案，以提高云计算平台的可信度量流程的透明度，增加用户对云计算平台的信任。

第一方面，本申请提供一种云计算平台的可信度量方法，所述方法包括：第三方管理和审计系统接收云计算平台中的软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心CA颁布的数字证书进行签名；所述第三方管理和审计系统从第三方测评机构获取所述软件的安全运行指标；所述第三方管理和审计系统根据经过所述数字证书签名的所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

通过可信的第三方管理和审计系统对云计算平台进行可信度量，并对云计算平台进行可信度量后得到的软件的原始的当前运行指标，与安全机构测评的该软件的安全运行指标进行比较，得到审计报告，使得云计算平台的可信度量过程公开，透明。避免了现有技术中，通过内部管理和审计系统对云计算平台进行可信度量的过程中，存在证书替换导致软件的当前运行指标可能被篡改的风险，提高了云计算平台的可信度量的真实性，从而提高用户对该云计算平台的信任。

结合第一方面，在第一方面的一种可能的实现方式中，所述软件的当前运行指标经过所述云计算平台采用所述CA颁布的数字证书进行签名。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，所述软件的当前运行指标携带所述云计算平台中的虚

拟机的标识，所述方法还包括：所述第三方管理和审计系统接收用户和虚拟机的标识的对应关系；所述第三方管理和审计系统根据所述虚拟机的标识，以及所述对应关系，确定所述虚拟机的标识对应的用户；所述第三方管理和审计系统向所述虚拟机的标识对应的用户发送所述审计报告。

通过在软件的当前运行指标中携带云计算平台中的虚拟机的标识，使得第三方管理和审计系统可以通过虚拟机的标识，将审计报告关联到使用该虚拟机的用户，从而使得每个用户可以获取与自身相关的审计报告。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，所述方法还包括：所述第三方管理和审计系统接收所述软件的运行版本信息；所述第三方管理和审计系统从所述第三方测评机构获取所述软件的测评版本信息；所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，包括：所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标、所述软件的运行版本信息以及所述软件的测评版本信息，生成审计报告。

通过第三方管理和审计系统从第三方安全测评机构获取软件的测评版本信息，将该软件的测评版本信息与云计算平台中该软件的运行版本信息，存储在审计报告中，该审计报告可以被用户获取，可以避免现有技术中，云计算平台的提供商将云计算平台中使用软件的运行版本和测评版本不一致的问题。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，所述方法还包括：所述第三方管理和审计系统接收所述云计算平台发送的所述云计算平台的运行日志；所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，还包括：所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标以及所述运行日志，生成所述审计报告。

通过第三方管理和审计系统将云计算平台中的运行日志，存储在审计报告中，供用户审计，使得该云计算平台的运行参数透明化，提高了用户对云计算平台的可信度。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，所述方法还包括：所述第三方管理和审计系统接收所述云计算平台发送的所述云计算平台的操作日志；所述第三方管理和审计系

统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，还包括：所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标以及所述操作日志，生成所述审计报告。

通过第三方管理和审计系统将云计算平台中的操作日志，存储在审计报告中，供用户审计，使得管理员对该云计算平台的相关操作透明化，提高了用户对云计算平台的可信度。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，在所述第三方管理和审计系统接收云计算平台中软件的当前运行指标之前，所述方法还包括：所述第三方管理和审计系统接收所述云计算平台发送的注册请求，所述注册请求包含所述云计算平台的数字证书；所述第三方管理和审计系统向所述云计算平台发送确认信息，所述确认信息表示所述云计算平台在所述第三方管理和审计系统中注册成功。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，在所述第三方管理和审计系统接收云计算平台中软件的当前运行指标之前，所述方法还包括：所述第三方管理和审计系统接收所述云计算平台发送的注册请求，所述注册请求包含所述可信平台的数字证书；所述第三方管理和审计系统向所述云计算平台发送确认信息，所述确认信息表示所述可信平台在所述第三方管理和审计系统中注册成功。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，所述方法还包括：所述第三方管理和审计系统向所述 CA 发送所述数字证书；所述第三方管理和审计系统接收所述 CA 发送的所述数字证书的验证信息，所述验证信息指示所述数字证书是否有效；所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，包括：所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标以及所述数字证书的验证信息，生成所述云平台系统的审计报告。

结合第一方面或其上述可能的实现方式中的任一种，在第一方面的另一种可能的实现方式中，所述第三方管理和审计系统为位于所述云计算平台之外的系统，且所述第三方管理和审计系统由可信的第三方提供，所述第三方管理和审计系统与所述云计算平台连接，且所述第三方管理和审计系统与所述第三方测评机构连接。

第三方管理和审计系统位于所述云计算平台之外的系统，且由可信的第三方提供，使得云计算平台的可信度量流程更加透明，提高了用户对云计算平台的可信度。

第二方面，本申请提供一种云计算平台的可信度量方法，所述方法包括：可信证据处理系统接收云计算平台中软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心CA颁布的数字证书进行签名；所述可信证据处理系统向第三方管理和审计系统发送所述软件的当前运行指标，以便于所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

通过可信的第三方管理和审计系统对云计算平台进行可信度量，并对云计算平台进行可信度量后得到的软件的原始的当前运行指标，与安全机构测评的该软件的安全运行指标进行比较，得到审计报告，使得云计算平台的可信度量过程公开，透明，避免了现有技术中，通过内部管理和审计系统对云计算平台进行可信度量的过程中，存在证书替换导致软件的当前运行指标可能被篡改的风险，提高了云计算平台的可信度量的真实性，从而提高用户对该云计算平台的信任。

结合第二方面，在第二方面的一种可能的实现方式中，在所述可信证据处理系统向第三方管理和审计系统发送所述软件的当前运行指标之前，所述方法还包括：可信证据处理系统通过所述云计算平台的数字证书对所述度量信息进行签名，且所述云计算平台的数字证书是所述CA颁布的数字证书。

结合第二方面或其上述可能的实现方式中的任一种，在第二方面的另一种可能的实现方式中，所述方法还包括：所述可信证据处理系统向所述第三方管理和审计系统发送用户和虚拟机的对应关系，以便于所述第三方管理和审计系统根据获取的虚拟机的标识信息确定用户，并向该用户发送所述审计报告。

通过向第三方管理和审计系统发送用户和虚拟机的对应关系，使得第三方管理和审计系统可以通过虚拟机的标识，将审计报告关联到使用该虚拟机的用户，从而使得每个用户可以获取与自身相关的审计报告。

结合第二方面或其上述可能的实现方式中的任一种，在第二方面的另一种可能的实现方式中，所述方法还包括：所述可信证据处理系统接收所述云

计算平台中所述软件的运行版本信息；所述可信证据处理系统向第三方管理和审计系统发送所述软件的运行版本信息。

通过可信证据处理系统向第三方管理和审计系统发送软件的运行版本，使得可以将该软件的测评版本与云计算平台中该软件的运行版本存储在审计报告中，被用户审计，可以避免现有技术中，云计算平台的提供商将云计算平台中使用软件的运行版本和测评版本不一致的问题。

结合第二方面或其上述可能的实现方式中的任一种，在第二方面的另一种可能的实现方式中，所述方法还包括：所述可行证据处理系统向所述 CA 发送所述可信平台的数字证书和所述云计算平台的数字证书；所述可行证据处理系统接收所述 CA 发送的验证信息，所述验证信息指示所述可信平台的数字证书和所述云计算平台的数字证书是否有效；所述可行证据处理系统向所述第三方管理和审计系统发送所述验证信息。

结合第二方面或其上述可能的实现方式中的任一种，在第二方面的另一种可能的实现方式中，在可信证据处理系统接收云计算平台中软件的当前运行指标之前，所述方法还包括：所述可行证据处理系统接收所述云计算平台发送的注册请求，所述注册请求包含云计算平台中可信平台的数字证书；所述可行证据处理系统向所述第三方管理和审计系统发送确认信息，所述确认信息表示所述可信平台在所述可行证据处理系统中注册成功。

结合第二方面或其上述可能的实现方式中的任一种，在第二方面的另一种可能的实现方式中，所述第三方管理和审计系统为位于所述云计算平台之外的系统，且所述第三方管理和审计系统由可信的第三方提供，所述第三方管理和审计系统与所述云计算平台连接，且所述第三方管理和审计系统与所述第三方安全测评机构连接。

第三方管理和审计系统位于所述云计算平台之外的系统，且由可信的第三方提供，使得云计算平台的可信度量流程更加透明，提高了用户对云计算平台的可信度。

第三方面，本申请提供一种云计算平台的可信度量装置，所述装置包括用于执行第一方面中的方法的模块。

第四方面，本申请提供一种云计算平台的可信度量装置，所述装置包括用于执行第二方面中的方法的模块。

第五方面，本申请提供一种计算机可读存储介质，所述计算机可读存储

介质用于存储云计算平台的可信度量的程序代码，所述程序代码用于执行第一方面中的方法指令。

第六方面，本申请提供一种计算机可读存储介质，所述计算机可读存储介质用于存储云计算平台的可信度量的程序代码，所述程序代码用于执行第二方面中的方法指令。

在某些实现方式中，软件的当前运行指标可以是该软件的完整性度量值，软件的安全运行指标可以是软件的完整性参考值。

在某些实现方式中，软件的当前运行指标可以包括软件可信启动度量信息、软件可信运行度量信息。

在某些实现方式中，可信证据处理系统可以为云计算平台中的处理模块。

本发明实施例通过第三方管理和审计系统，对云计算平台的可信度量信息进行审计，并且审计报告可被用户审计，使得云计算平台的可信度量过程公开、透明，提高了云计算平台的可信度量的真实性，从而提高了用户对云计算平台的信任。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例中所需要使用的附图作简单地介绍，显而易见地，下面所描述的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是现有技术中对云计算平台进行可信度量的架构的示意图。

图 2 是根据本发明实施例的云计算平台的可信度量方法的示意性流程图。

图 3 是本发明实施例的云计算平台的可信度量装置的示意性框图。

图 4 是本发明实施例的云计算平台的可信度量装置的示意性框图。

图 5 本发明实施例的云计算平台的可信度量装置的示意性框图。

图 6 本发明实施例的云计算平台的可信度量装置的示意性框图。

具体实施方式

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，所描述的实施例是本发明一部分实施例，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作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

TCG 对“可信”的定义是：“一个实体在实现给定目标时，若其行为总是如同预期，则该实体是可信的”。这个定义将可信计算和当前的安全技术分开：可信强调行为结果可预期，但并不等于确认行为是安全的，这是两个不同的概念。例如，用户知道自己的电脑中有病毒，这些病毒会在什么时候发作，并且了解会产生的后果，同时病毒也确实是这么运行的，那么这台电脑就是可信的。从 TCG 的定义来看，可信实际上还包含了容错计算里可靠性的概念。可靠性保证硬件或者软件系统性能可预测。

现有技术中，为了提高用户对云计算平台的信任感，在验证服务器与云计算平台建立信任的过程中引入可信计算技术。可信计算技术的重要应用是保护软件的完整性，TPM 安全芯片是可信计算的关键部件，它以密码技术为核心，具有计算与存储功能，支持数据保护、身份证明和完整性度量等，可对软件进行完整性度量并提供度量报告，在物理安全方面具有防攻击、防篡改、防探测的能力，可以保证 TPM 自身以及内部数据不被非法攻击。在技术安全方面，TPM 采用了多种密码和访问控制技术。在管理安全方面，TPM 在中国属于商用密码产品，其研制、生产、销售和使用都按国家商用密码产品进行有效管理。这些保护措施共同确保了 TPM 自身的安全，从而可以成为云计算平台的硬件存储信任根和云计算平台可信的基点。

云计算平台节点可以以部署在 BIOS 或者 CPU 中的 TPM 安全芯片为信任根，遵从“先度量，再执行”的原则，一级度量认证一级，一级信任一级，建立一条从 TPM 安全芯片到云计算平台的操作系统，再由操作系统到运行软件的信任链，从而实现对云计算平台的可信度量。

为了避免现有技术中，提供商可能会替换内部数字证书，导致的度量信息存在被篡改的这一风险，在对云计算平台进行可信度量之后，可以将可信度量报告发送到第三方管理和审计系统，通过第三方管理和审计系统生成的审计报告，提高用户对云计算平台的信任感。下面结合图 2，详细描述根据本发明实施例的云计算平台的可信度量方法。

图 2 是根据本发明实施例的云计算平台的可信度量方法的示意性流程图。应理解，图 2 示出了云计算平台的可信度量方法的详细的步骤或操作，

但这些步骤或操作仅是示例，本发明实施例还可以执行其他操作，或者图 2 中各操作的变形。此外，图 2 中的各个步骤可以按照与图 2 呈现的不同顺序来执行，并且有可能并非要执行图 2 中的全部操作。下面具体描述图 2 所示的方法步骤。

210、第三方管理和审计系统接收云计算平台发送的注册请求，完成可信证据处理系统到第三方管理和审计系统的注册过程。

具体地，注册请求包含云平台数字证书和可信平台数字证书。第三方管理和审计系统可以接收云计算平台中的可信证据处理系统发送的2次注册请求，2 次注册请求分别包含云计算平台数字证书和可信平台数字证书；第三方管理和审计系统还可以接收云计算平台中的可信证据处理系统发送的1次注册请求，该注册请求同时包含云计算平台数字证书和可信平台数字证书。

220、第三方管理和审计系统向 CA 发送云计算平台的数字证书和可信平台的数字证书。

具体地，第三方管理和审计系统向 CA 发送云计算平台的数字证书和可信平台的数字证书，以验证上述数字证书的有效性。

230、可信证据处理系统向第三方管理和审计系统发送用户和虚拟机标识的对应关系。

240、计算节点向可信证据处理系统发送云计算平台中软件的当前运行指标和软件的运行版本信息。

具体地，软件的当前运行指标经过可信平台的数字证书进行签名，且可信平台在签名软件的度量信息时采用的数字证书是 CA 颁布的数字证书。

可选地，计算节点向可信证据处理系统还可以发送云计算平台的运行日志以及云计算平台的操作日志。

应理解，上述软件的当前运行指标可以包括软件启动度量数据、软件运行度量数据。由于上述软件的当前运行指标中度量数据的种类不同，计算节点向可信证据处理系统发送度量信息的时间周期也可以不同，例如，软件的启动度量数据可以在该软件启动后，直接向可信证据处理系统发送，发送次数可以为 1；软件的运行度量数据可以在对该软件的运行状态进行度量后，以预设周期向可信证据处理系统发送。云计算平台的运行日志和云计算平台的操作日志也可以采用和软件运行度量数据相同的方式，向可信证据处理系统发送。

还应理解，为了第三方管理和审计系统在性能优先的工作模式下工作，可行证据处理系统还可以将计算节点发送的软件的当前运行指标进行存储，然后在同一时间向第三方管理和审计系统发送。

250、第三方管理和审计系统接收可信证据处理系统发送的软件的当前运行指标软件的度量信息携带虚拟机标识信息。

可选地，在一个实施例中，上述软件的当前运行指标还可以经过云平台数字证书进行签名。

260、第三方管理和审计系统接收第三方测评机构发送的软件的安全运行指标和软件的测评版本信息。

可选地，在一个实施例中，软件的测评信息可以包括该软件的数字指纹。

270、第三方管理和审计系统根据软件的当前运行指标、软件的安全运行指标、软件的运行版本信息和软件的测评版本信息，生成审计报告。

应理解，上述审计报告可以由第三方管理和审计系统发送给虚拟机标识对应的用户，或者由第三方管理和审计系统发送在审计报告的公告栏中，用户可以自己查阅，本发明对此不作具体限定。

上文结合图 1 和图 2 详细的描述了本发明实施例的云计算平台的可信度量方法，下面结合图 3 至图 6，详细描述本发明实施例的云计算平台的可信度量装置。应理解，图 3 至图 6 所示的装置能够实现图 2 中的各个步骤，为避免重复，在此不再详细赘述。

图 3 是本发明实施例的云计算平台的可信度量装置的示意性框图。图 3 所示的装置 300 包括第一接收模块 310、第一获取模块 320、生成模块 330。

第一接收模块 310，用于接收云计算平台中的软件当前运行指标，所述度量信息经过所述云计算平台中的可信平台采用证书授权中心 CA 颁布的数字证书进行签名；

第一获取模块 320，用于从第三方测评机构获取所述软件的安全运行指标；

生成模块 330，用于根据所述接收模块接收的所述软件的当前运行指标和所述获取模块获取的所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

通过可信的第三方管理和审计系统对云计算平台进行可信度量，并对云计算平台进行可信度量后得到的软件的原始的当前运行指标，与安全机构测

评的该软件的安全运行指标进行比较，得到审计报告，使得云计算平台的可信度量过程公开，透明，避免了现有技术中，通过内部管理和审计系统对云计算平台进行可信度量的过程中，存在证书替换导致软件的当前运行指标可能被篡改的风险，提高了云计算平台的可信度量的真实性，从而提高用户对该云计算平台的信任。

图 4 是本发明实施例的云计算平台的可信度量装置的示意性框图。图 4 所示的装置 400 包括第一接收模块 410 和第一发送模块 420。

第一接收模块 410，用于接收云计算平台中软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心 CA 颁布的数字证书进行签名；

第一发送模块 420，用于向第三方管理和审计系统发送所述软件的当前运行指标，以便于所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

通过可信的第三方管理和审计系统对云计算平台进行可信度量，并对云计算平台进行可信度量后得到的软件的原始的当前运行指标，与安全机构测评的该软件的安全运行指标进行比较，得到审计报告，使得云计算平台的可信度量过程公开，透明，避免了现有技术中，通过内部管理和审计系统对云计算平台进行可信度量的过程中，存在证书替换导致软件的当前运行指标可能被篡改的风险，提高了云计算平台的可信度量的真实性，从而提高用户对该云计算平台的信任。

图 5 是本发明实施例的云计算平台的可信度量装置的示意性框图。图 5 所示的装置 500 包括：存储器 510、处理器 520、输入/输出接口 530、通信接口 540 和总线系统 550。其中，存储器 510、处理器 520、输入/输出接口 530 和通信接口 540 通过总线系统 550 相连，该存储器 510 用于存储指令，该处理器 520 用于执行该存储器 520 存储的指令，以控制输入/输出接口 530 接收输入的数据和信息，输出操作结果等数据，并控制通信接口 540 发送信号。

通信接口 540，用于接收云计算平台中的软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心 CA 颁布的数字证书进行签名；从第三方测评机构获取所述软件的安全运行指

标;

处理器 520，用于根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

应理解，在本发明实施例中，该处理器 520 可以采用通用的中央处理器（Central Processing Unit，CPU），微处理器，应用专用集成电路（Application Specific Integrated Circuit，ASIC），或者一个或多个集成电路，用于执行相关程序，以实现本发明实施例所提供的技术方案。

还应理解，通信接口 540 使用例如但不限于收发器一类的收发装置，来实现移动终端 500 与其他设备或通信网络之间的通信。

该存储器 510 可以包括只读存储器和随机存取存储器，并向处理器 520 提供指令和数据。处理器 520 的一部分还可以包括非易失性随机存取存储器。例如，处理器 520 还可以存储设备类型的信息。

该总线系统 550 除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线系统 550。

在实现过程中，上述方法的各步骤可以通过处理器 520 中的硬件的集成逻辑电路或者软件形式的指令完成。结合本发明实施例所公开的可信度量的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 510，处理器 520 读取存储器 510 中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

通过可信的第三方管理和审计系统对云计算平台进行可信度量，并对云计算平台进行可信度量后得到的软件的原始的当前运行指标，与安全机构测评的该软件的安全运行指标进行比较，得到审计报告，使得云计算平台的可信度量过程公开，透明，避免了现有技术中，通过内部管理和审计系统对云计算平台进行可信度量的过程中，存在证书替换导致软件的当前运行指标可能被篡改的风险，提高了云计算平台的可信度量的真实性，从而提高用户对该云计算平台的信任。

图 6 本发明实施例的云计算平台的可信度量装置的示意性框图。图 6 所示的装置 600 包括：存储器 610、处理器 620、输入/输出接口 630、通信接

口 640 和总线系统 650。其中，存储器 610、处理器 620、输入/输出接口 630 和通信接口 640 通过总线系统 650 相连，该存储器 610 用于存储指令，该处理器 620 用于执行该存储器 620 存储的指令，以控制输入/输出接口 630 接收输入的数据和信息，输出操作结果等数据，并控制通信接口 640 发送信号。

通信接口 640，用于接收云计算平台中软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心 CA 颁布的数字证书进行签名；向第三方管理和审计系统发送所述软件的当前运行指标，以便于所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

应理解，在本发明实施例中，该处理器 620 可以采用通用的中央处理器（Central Processing Unit，CPU），微处理器，应用专用集成电路（Application Specific Integrated Circuit，ASIC），或者一个或多个集成电路，用于执行相关程序，以实现本发明实施例所提供的技术方案。

还应理解，通信接口 640 使用例如但不限于收发器一类的收发装置，来实现移动终端 600 与其他设备或通信网络之间的通信。

该存储器 610 可以包括只读存储器和随机存取存储器，并向处理器 620 提供指令和数据。处理器 620 的一部分还可以包括非易失性随机存取存储器。例如，处理器 620 还可以存储设备类型的信息。

该总线系统 650 除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线系统 650。

在实现过程中，上述方法的各步骤可以通过处理器 620 中的硬件的集成逻辑电路或者软件形式的指令完成。结合本发明实施例所公开的可信度量方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 610，处理器 620 读取存储器 610 中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

通过可信的第三方管理和审计系统对云计算平台进行可信度量，并对云计算平台进行可信度量后得到的软件的原始的当前运行指标，与安全机构测

评的该软件的安全运行指标进行比较，得到审计报告，使得云计算平台的可信度量过程公开，透明，避免了现有技术中，通过内部管理和审计系统对云计算平台进行可信度量的过程中，存在证书替换导致软件的当前运行指标可能被篡改的风险，提高了云计算平台的可信度量的真实性，从而提高用户对该云计算平台的信任。

应理解，在本发明实施例中，“与 A 相应的 B”表示 B 与 A 相关联，根据 A 可以确定 B。但还应理解，根据 A 确定 B 并不意味着仅仅根据 A 确定 B，还可以根据 A 和/或其它信息确定 B。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

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。

所述功能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时，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（可以是个人计算机，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、移动硬盘、只读存储器(Read-Only Memory, ROM)、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述或该，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

权利要求

1、一种云计算平台的可信度量方法，其特征在于，包括:

第三方管理和审计系统接收云计算平台中的软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心CA颁布的数字证书进行签名;

所述第三方管理和审计系统从第三方测评机构获取所述软件的安全运行指标;

所述第三方管理和审计系统根据经过所述数字证书签名的所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

2、如权利要求 1 所述的方法，其特征在于，所述软件的当前运行指标经过所述云计算平台采用所述CA颁布的数字证书进行签名。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述软件的当前运行指标携带所述云计算平台中的虚拟机的标识，所述方法还包括:

所述第三方管理和审计系统接收用户和虚拟机的标识的对应关系;

所述第三方管理和审计系统根据所述虚拟机的标识，以及所述对应关系，确定所述虚拟机的标识对应的用户;

所述第三方管理和审计系统向所述虚拟机的标识对应的用户发送所述审计报告。

4、如权利要求 1 至 3 中任一项所述的方法，其特征在于，所述方法还包括:

所述第三方管理和审计系统接收所述软件的运行版本信息;

所述第三方管理和审计系统从所述第三方测评机构获取所述软件的测评版本信息;

所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，包括:

所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标、所述软件的运行版本信息以及所述软件的测评版本信息，生成审计报告。

5、如权利要求 1 至 4 中任一项所述的方法，其特征在于，所述方法还包括:

所述第三方管理和审计系统接收所述云计算平台发送的所述云计算平台的运行日志;

所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，还包括:

所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标以及所述运行日志，生成所述审计报告。

6、如权利要求 1 至 5 中任一项所述的方法，其特征在于，所述方法还包括:

所述第三方管理和审计系统接收所述云计算平台发送的所述云计算平台的操作日志;

所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，还包括:

所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标以及所述操作日志，生成所述审计报告。

7、如权利要求 1 至 6 中任一项所述的方法，其特征在于，在所述第三方管理和审计系统接收云计算平台中软件的当前运行指标之前，所述方法还包括:

所述第三方管理和审计系统接收所述云计算平台发送的注册请求，所述注册请求包含所述云计算平台的数字证书;

所述第三方管理和审计系统向所述云计算平台发送确认信息，所述确认信息表示所述云计算平台在所述第三方管理和审计系统中注册成功。

8、如权利要求 1 至 7 中任一项所述的方法，其特征在于，在所述第三方管理和审计系统接收云计算平台中软件的当前运行指标之前，所述方法还包括:

所述第三方管理和审计系统接收所述云计算平台发送的注册请求，所述注册请求包含所述可信平台的数字证书;

所述第三方管理和审计系统向所述云计算平台发送确认信息，所述确认信息表示所述可信平台在所述第三方管理和审计系统中注册成功。

9、如权利要求 1 至 8 中任一项所述的方法，其特征在于，所述方法还包括:

所述第三方管理和审计系统向所述 CA 发送所述数字证书;

所述第三方管理和审计系统接收所述CA发送的所述数字证书的验证信息，所述验证信息指示所述数字证书是否有效；

所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，包括：

所述第三方管理和审计系统根据所述软件的当前运行指标、所述软件的安全运行指标以及所述数字证书的验证信息，生成所述审计报告。

10、如权利要求1至9中任一项所述的方法，其特征在于，所述第三方管理和审计系统为位于所述云计算平台之外的系统，且所述第三方管理和审计系统由可信的第三方提供，所述第三方管理和审计系统与所述云计算平台连接，且所述第三方管理和审计系统与所述第三方测评机构连接。

11、一种云计算平台的可信度量方法，其特征在于，包括：

可信证据处理系统接收云计算平台中软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心CA颁布的数字证书进行签名；

所述可信证据处理系统向第三方管理和审计系统发送所述软件的当前运行指标，以便于所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

12、如权利要求11所述的方法，其特征在于，在所述可信证据处理系统向第三方管理和审计系统发送所述软件的当前运行指标之前，所述方法还包括：

可信证据处理系统通过所述云计算平台的数字证书对所述当前运行指标进行签名，且所述云计算平台的数字证书是所述CA颁布的数字证书。

13、如权利要求11或12所述的方法，其特征在于，所述方法还包括：

所述可信证据处理系统向所述第三方管理和审计系统发送用户和虚拟机的对应关系，以便于所述第三方管理和审计系统根据获取的虚拟机的标识信息确定用户，并向该用户发送所述审计报告。

14、如权利要求11至13中任一项所述的方法，其特征在于，所述方法还包括：

所述可信证据处理系统接收所述云计算平台中所述软件的运行版本信息；

所述可信证据处理系统向第三方管理和审计系统发送所述软件的运行版本信息。

15、如权利要求 11 至 14 中任一项所述的方法，其特征在于，所述方法还包括:

所述可信证据处理系统向所述CA发送所述可信平台的数字证书和所述云计算平台的数字证书;

所述可信证据处理系统接收所述CA发送的验证信息，所述验证信息指示所述可信平台的数字证书和所述云计算平台的数字证书是否有效;

所述可信证据处理系统向所述第三方管理和审计系统发送所述验证信息。

16、如权利要求 11 至 15 中任一项所述的方法，其特征在于，在可信证据处理系统接收云计算平台中软件的当前运行指标之前，所述方法还包括:

所述可信证据处理系统接收所述云计算平台发送的注册请求，所述注册请求包含云计算平台中可信平台的数字证书;

所述可信证据处理系统向所述第三方管理和审计系统发送确认信息，所述确认信息表示所述可信平台在所述可行证据处理系统中注册成功。

17、如权利要求 11 至 16 中任一项所述的方法，其特征在于，所述第三方管理和审计系统为位于所述云计算平台之外的系统，且所述第三方管理和审计系统由可信的第三方提供，所述第三方管理和审计系统与所述云计算平台连接，且所述第三方管理和审计系统与所述第三方安全测评机构连接。

18、一种云计算平台的可信度量装置，其特征在于，包括:

第一接收模块，用于接收云计算平台中的软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心 CA 颁布的数字证书进行签名;

第一获取模块，用于从第三方测评机构获取所述软件的安全运行指标;

生成模块，用于根据所述接收模块接收的经过所述数字证书签名的所述软件的当前运行指标，和所述获取模块获取的所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

19、如权利要求 18 所述的装置，其特征在于，所述软件的当前运行指标经过所述云计算平台采用所述CA颁布的数字证书进行签名。

20、如权利要求 18 或 19 所述的装置，其特征在于，所述软件的当前运

行指标携带所述云计算平台中的虚拟机的标识，所述装置还包括:

第二接收模块，用于接收用户和虚拟机的标识的对应关系;

确定模块，用于根据所述虚拟机的标识，以及所述对应关系，确定所述虚拟机的标识对应的用户;

第一发送模块，用于向所述虚拟机的标识对应的用户发送所述审计报告。

21、如权利要求 18 至 20 中任一项所述的装置，其特征在于，所述装置还包括:

第三接收模块，用于接收所述软件的运行版本信息;

第二获取模块，用于从所述第三方测评机构获取所述软件的测评版本信息;

所述生成模块，还用于根据所述软件的当前运行指标、所述软件的安全运行指标、所述软件的运行版本以及所述软件的测评版本，生成审计报告。

22、如权利要求 18 至 21 中任一项所述的装置，其特征在于，所述装置还包括:

第四接收模块，用于接收所述云计算平台发送的所述云计算平台的运行日志;

所述生成模块，还用于根据所述软件的当前运行指标、所述软件的安全运行指标以及所述运行日志，生成所述审计报告。

23、如权利要求 18 至 22 中任一项所述的方法，其特征在于，所述装置还包括:

第五接收模块，用于接收所述云计算平台发送的所述云计算平台的操作日志;

所述生成模块，还用于根据所述软件的当前运行指标、所述软件的安全运行指标以及所述操作日志，生成所述审计报告。

24、如权利要求 18 至 23 中任一项所述的装置，其特征在于，所述装置还包括:

第四接收模块，用于接收所述云计算平台发送的注册请求，所述注册请求包含所述云计算平台的数字证书;

第二发送模块，用于向所述云计算平台发送确认信息，所述确认信息表示所述云计算平台在所述第三方管理和审计系统中注册成功。

25、如权利要求 18 至 24 中任一项所述的装置，其特征在于，所述装置还包括:

第五接收模块，用于接收所述云计算平台发送的注册请求，所述注册请求包含所述可信平台的数字证书;

第三发送模块，用于向所述云计算平台发送确认信息，所述确认信息表示所述可信平台在所述第三方管理和审计系统中注册成功。

26、如权利要求 18 至 25 中任一项所述的装置，其特征在于，所述装置还包括:

第四发送模块，用于向所述 CA 发送所述数字证书;

第六接收模块，用于接收所述 CA 发送的所述数字证书的验证信息，所述验证信息指示所述数字证书是否有效;

所述生成模块，还用于根据所述软件的当前运行指标、所述软件的安全运行指标以及所述数字证书的验证信息，生成所述审计报告。

27、如权利要求 18 至 26 中任一项所述的装置，其特征在于，所述第三方管理和审计系统为位于所述云计算平台之外的系统，且所述第三方管理和审计系统由可信的第三方提供，所述第三方管理和审计系统与所述云计算平台连接，且所述第三方管理和审计系统与所述第三方测评机构连接。

28、一种云计算平台的可信度量装置，其特征在于，包括:

第一接收模块，用于接收云计算平台中软件的当前运行指标，所述软件的当前运行指标经过所述云计算平台中的可信平台采用证书授权中心 CA 颁布的数字证书进行签名;

第一发送模块，用于向第三方管理和审计系统发送所述软件的当前运行指标，以便于所述第三方管理和审计系统根据所述软件的当前运行指标和所述软件的安全运行指标，生成审计报告，所述审计报告用于指示所述云计算平台的可信度。

29、如权利要求 28 所述的装置，其特征在于，所述装置还包括:

处理模块，用于通过所述云计算平台的数字证书对所述当前运行指标进行签名，且所述云计算平台的数字证书是所述 CA 颁布的数字证书。

30、如权利要求 28 或 29 所述的装置，其特征在于，所述装置还包括:

第二发送模块，用于向所述第三方管理和审计系统发送用户和虚拟机的对应关系，以便于所述第三方管理和审计系统根据获取的虚拟机的标识信息

确定用户，并向该用户发送所述审计报告。

31、如权利要求 28 至 30 中任一项所述的装置，其特征在于，所述装置还包括:

第二接收模块，用于接收所述云计算平台中软件的运行版本信息;

第三发送模块，用于向第三方管理和审计系统发送所述软件的运行版本信息。

32、如权利要求 28 至 31 中任一项所述的装置，其特征在于，所述装置还包括:

第四发送模块，用于向所述 CA 发送所述可信平台的数字证书和所述云计算平台的数字证书;

第三接收模块，用于接收所述 CA 发送的验证信息，所述验证信息指示所述可信平台的数字证书和所述云计算平台的数字证书是否有效;

第五发送模块，用于向所述第三方管理和审计系统发送所述验证信息。

33、如权利要求 28 至 32 中任一项所述的装置，其特征在于，所述装置还包括:

第四接收模块，用于接收所述云计算平台发送的注册请求，所述注册请求包含云计算平台中可信平台的数字证书;

第六发送模块，用于向所述第三方管理和审计系统发送确认信息，所述确认信息表示所述可信平台在所述可行证据处理系统中注册成功。

34、如权利要求 28 至 33 中任一项所述的装置，其特征在于，所述第三方管理和审计系统为位于所述云计算平台之外的系统，且所述第三方管理和审计系统由可信的第三方提供，所述第三方管理和审计系统与所述云计算平台连接，且所述第三方管理和审计系统与所述第三方测评机构连接。

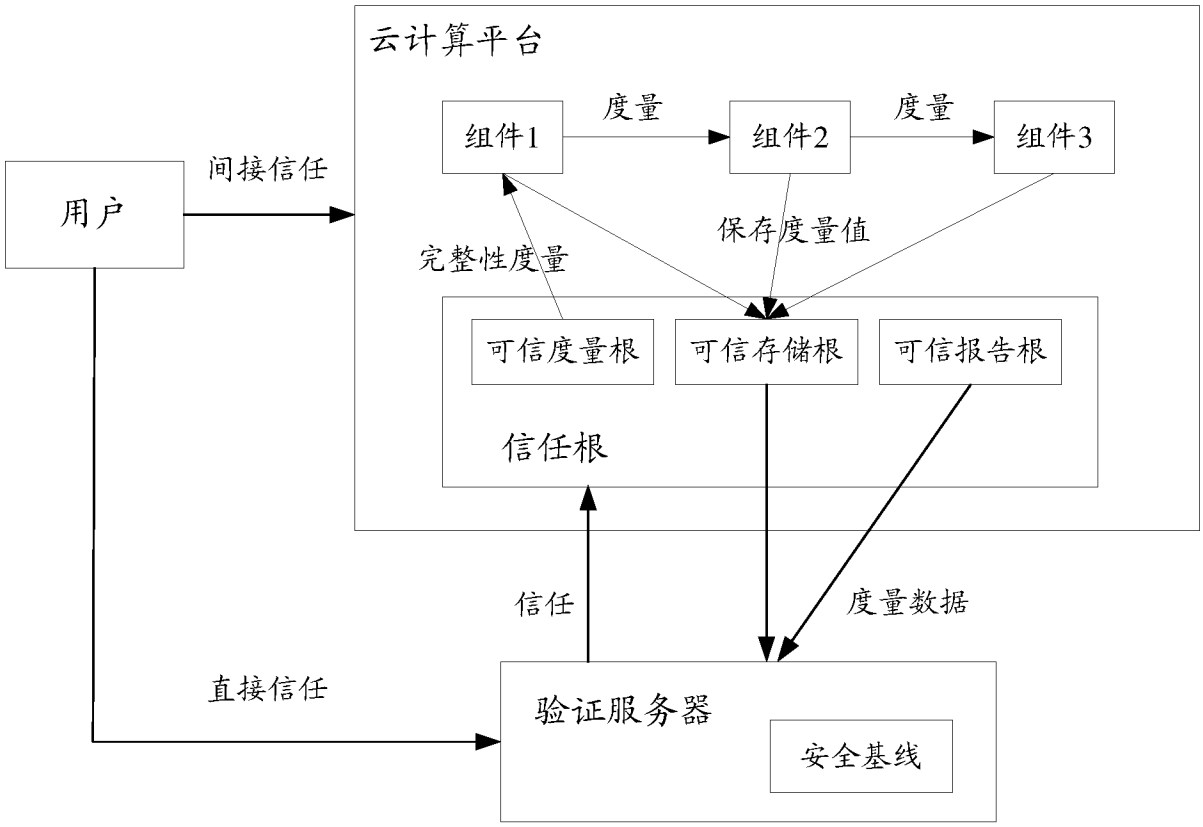
云计算平台
组件1
度量
组件2
度量
组件3
用户
间接信任
保存度量值
完整性度量
可信度量根
可信存储根
可信报告根
信任根
信任
度量数据
直接信任
验证服务器
安全基线

图 1

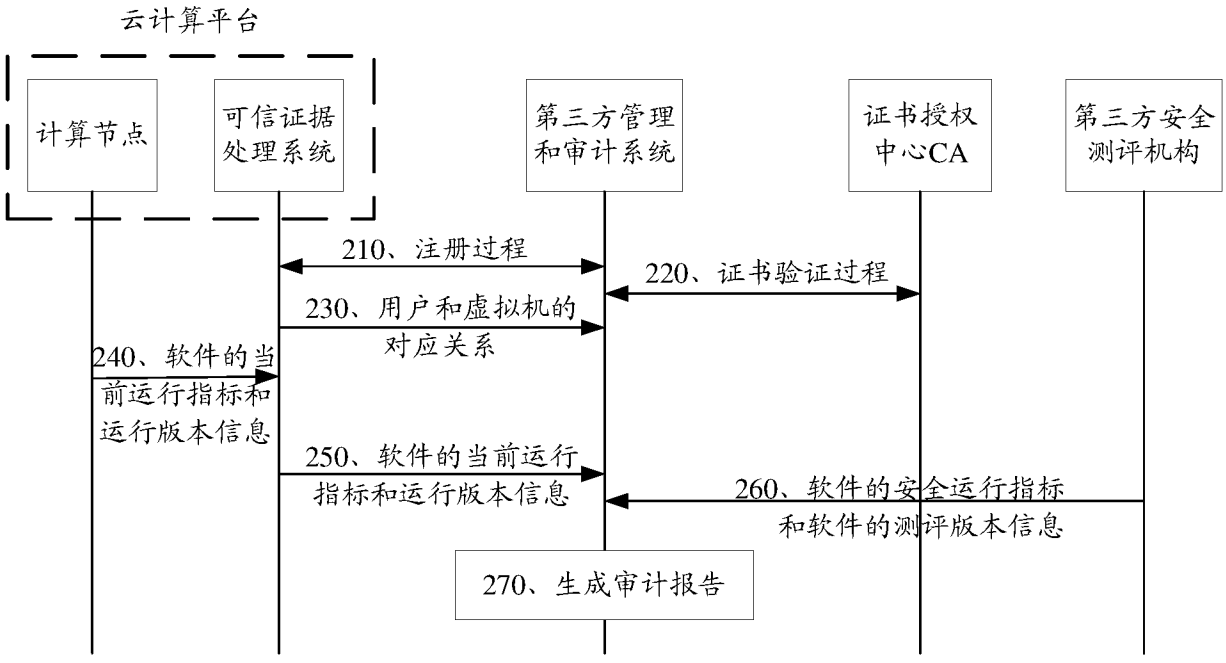
云计算平台
计算节点
可信证据处理系统
第三方管理和审计系统
证书授权中心CA
第三方安全测评机构
210、注册过程
220、证书验证过程
230、用户和虚拟机的对应关系
240、软件的当前运行指标和运行版本信息
250、软件的当前运行指标和运行版本信息
260、软件的安全运行指标和软件的测评版本信息
270、生成审计报告

图 2

装置300
第一接收模块310
第一获取模块320
生成模块330

图 3

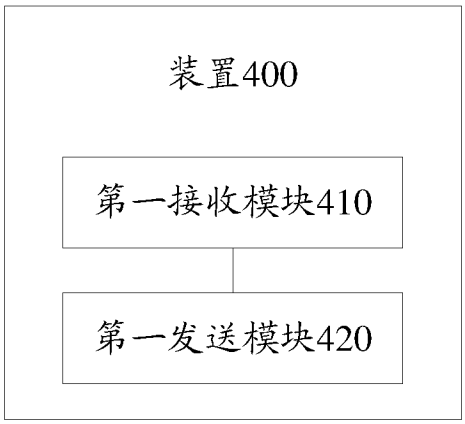
装置400
第一接收模块410
第一发送模块420

图 4

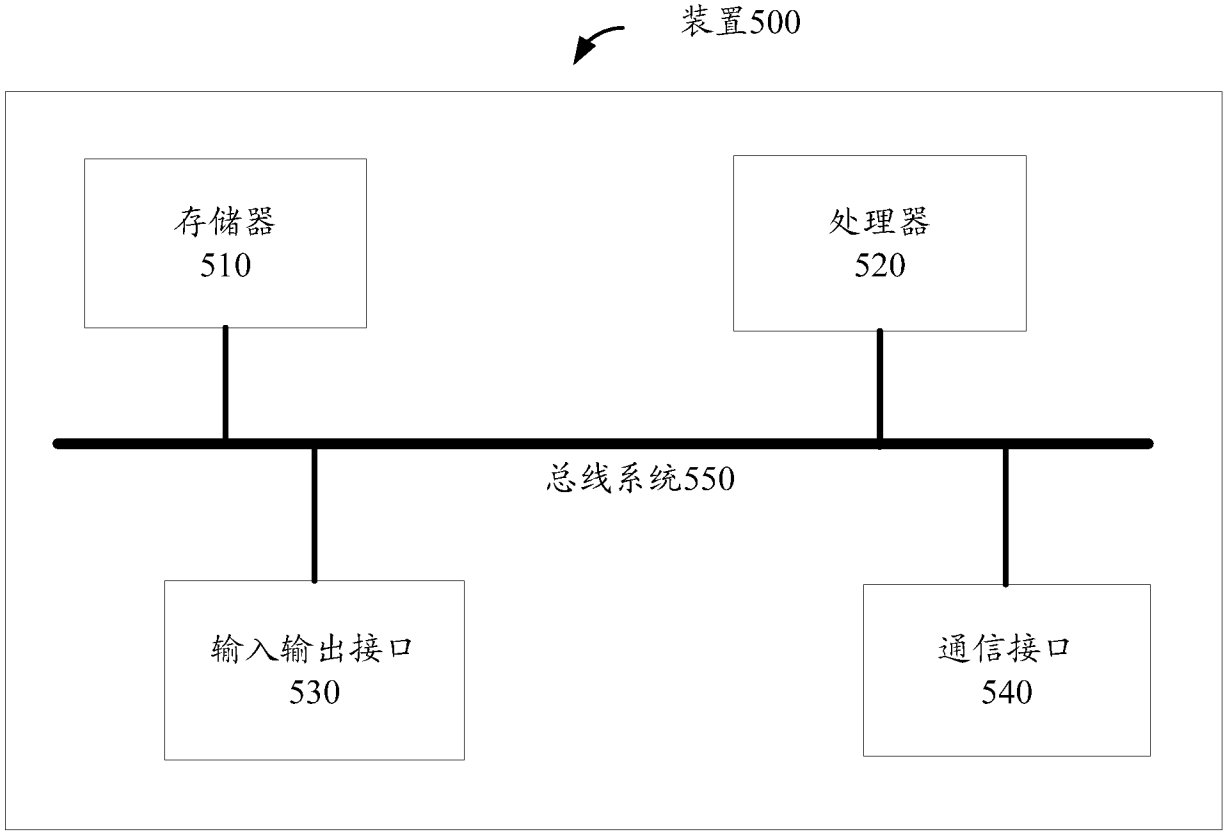

图 5

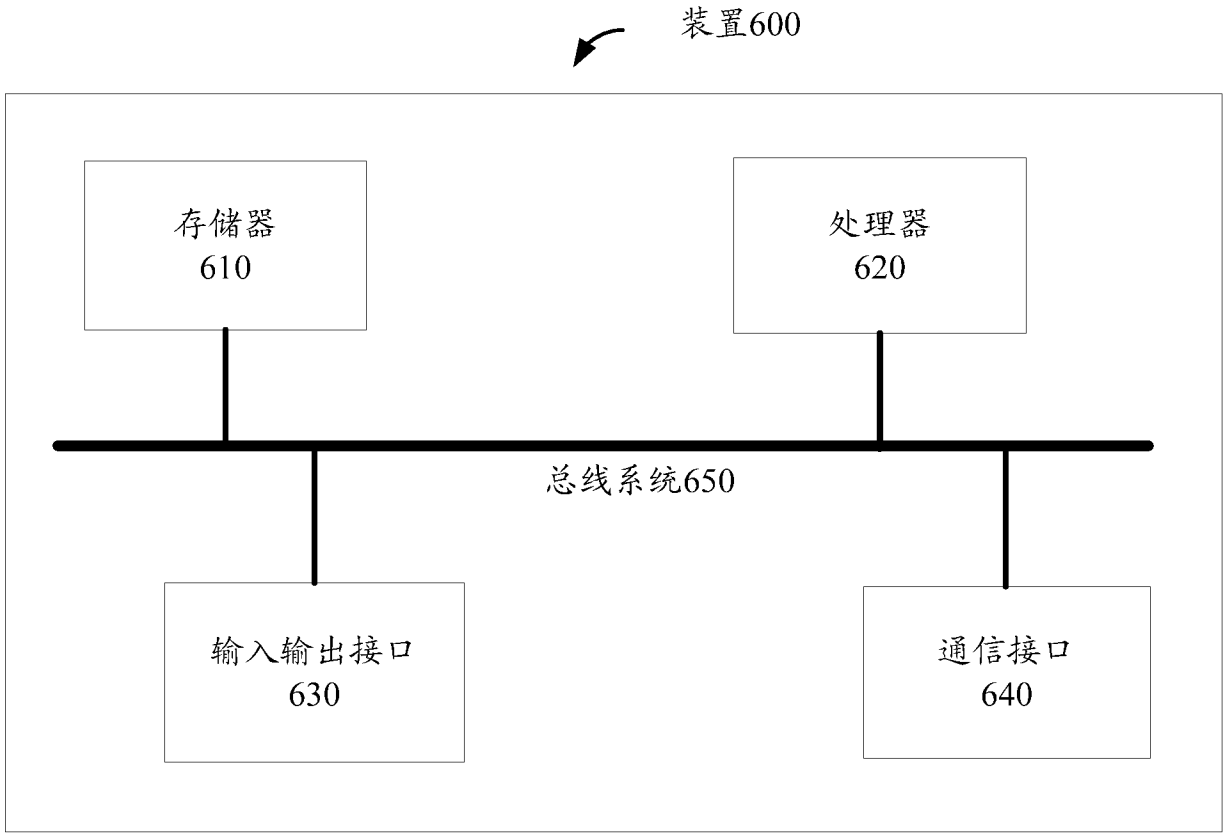

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/097668

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, EPODOC, WPI, GOOGLE, CNKI: credible, cloud platform, TPM, cloud computing, trust, measure, evaluate, audit, third party, certification, authority, CA, signature, report, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101043338 A (INSTITUTE OF SOFTWARE, CHINESE ACADEMY OF SCIENCES), 26 September 2007 (26.09.2007), description, page 2, paragraph 3 to page 4, paragraph 4, and figures 1-4	1-2, 18-19
Y	CN 101043338 A (INSTITUTE OF SOFTWARE, CHINESE ACADEMY OF SCIENCES), 26 September 2007 (26.09.2007), description, page 2, paragraph 3 to page 4, paragraph 4, and figures 1-4	3-17, 20-34
Y	LIANG, Lulu et al. "A Trusted Evaluation Framework for Cloud Platform Based on Trusted Third Party", PROCEEDINGS OF THE 7TH CONFERENCE ON VULNERABILITY ANALYSIS AND RISK ASSESSMENT, 23 April 2015 (23.04.2015), section 4.3, and figure 3	11-17, 28-34
Y	CN 103843303 A (HUAWEI TECHNOLOGIES CO., LTD.), 04 June 2014 (04.06.2014), description, paragraphs [0068] and [0097], and figures 2 and 3	3-10, 13-17, 20-27, 30-34
A	CN 101477602 A (INSPUR ELECTRONIC INFORMATION INDUSTRY CO., LTD.), 08 July 2009 (08.07.2009), the whole document	1-34
A	CN 101242297 A (CHINA INSTANT WIRELESS NETWORK COMMUNICATIONS CO., LTD.), 13 August 2008 (13.08.2008), the whole document	1-34

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 November 2016 (22.11.2016)	**06 December 2016 (06.12.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **GUO, Minghua** Telephone No.: (86-10) **62414092**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/097668

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2014039497 A1 (AMRITA VISHWA VIDYAPEETHAM), 13 March 2014 (13.03.2014), the whole document	1-34

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/097668

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101043338 A	26 September 2007	CN 100583768 C	20 January 2010
CN 103843303 A	04 June 2014	US 2015256341 A1	10 September 2015
		WO 2014079009 A1	30 May 2014
		JP 2016506107 A	25 February 2016
		EP 2913956 A1	02 September 2015
CN 101477602 A	08 July 2009	None	
CN 101242297 A	13 August 2008	KR 20110128370 A	29 November 2011
		KR 20100017951 A	16 February 2010
		KR 101135346 B1	17 April 2012
		US 2010083349 A1	01 April 2010
		WO 2009033385 A1	19 March 2009
		US 8230220 B2	24 July 2012
		CN 100581116 C	13 January 2010
WO 2014039497 A1	13 March 2014	US 2014075568 A1	13 March 2014

国际检索报告

国际申请号
PCT/CN2016/097668

A. 主题的分类

G06F 21/57(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT，EPODOC，WPI，GOOGLE，CNKI：云计算，云平台，可信，度量，测评，评测，审计，第三方，证书，认证，签名，报告，安全，cloud platform，TPM，cloud computing，trust，measure，evaluate，audit，third party，certification，authority，CA，signature，report，security

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 101043338 A (中国科学院软件研究所) 2007年 9月 26日 (2007 - 09 - 26) 说明书第2页第3段至第4页第4段，图1-4	1-2,18-19
Y	CN 101043338 A (中国科学院软件研究所) 2007年 9月 26日 (2007 - 09 - 26) 说明书第2页第3段至第4页第4段，图1-4	3-17,20-34
Y	梁露露 等,. "基于第三方的可信评测框架," 第七届信息安全漏洞分析与风险评估大会论文集，2015年 4月 23日 (2015 - 04 - 23)， 第4.3节，图3	11-17,28-34
Y	CN 103843303 A (华为技术有限公司) 2014年 6月 4日 (2014 - 06 - 04) 说明书第[0068]，[0097]段，图2，3	3-10,13-17, 20-27,30-34
A	CN 101477602 A (浪潮电子信息产业股份有限公司) 2009年 7月 8日 (2009 - 07 - 08) 全文	1-34
A	CN 101242297 A (西安西电捷通无线网络通信有限公司) 2008年 8月 13日 (2008 - 08 - 13) 全文	1-34

☑ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 11月 22日	2016年 12月 6日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 郭明华 电话号码 (86-10)62414092

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	WO 2014039497 A1 (AMRITA VISHWA VIDYAPEETHAM) 2014年 3月 13日 (2014-03-13) 全文	1-34

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/097668

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101043338	A	2007年 9月 26日	CN	100583768	C	2010年 1月 20日
CN	103843303	A	2014年 6月 4日	US	2015256341	A1	2015年 9月 10日
				WO	2014079009	A1	2014年 5月 30日
				JP	2016506107	A	2016年 2月 25日
				EP	2913956	A1	2015年 9月 2日
CN	101477602	A	2009年 7月 8日		无		
CN	101242297	A	2008年 8月 13日	KR	20110128370	A	2011年 11月 29日
				KR	20100017951	A	2010年 2月 16日
				KR	101135346	B1	2012年 4月 17日
				US	2010083349	A1	2010年 4月 1日
				WO	2009033385	A1	2009年 3月 19日
				US	8230220	B2	2012年 7月 24日
				CN	100581116	C	2010年 1月 13日
WO	2014039497	A1	2014年 3月 13日	US	2014075568	A1	2014年 3月 13日