可信云平台技术综述

何欣枫[1,2,3]，田俊峰[1,2,3]，刘凡鸣[2,3]

（1. 河北大学管理学院，河北 保定 071002；2. 河北大学网络空间安全与计算机学院，河北 保定 071002；
3. 河北省高可信信息系统重点实验室，河北 保定 071002）

摘 要：云计算安全需求使信息安全技术面临更严峻的挑战，云平台自身的可信性是保证云计算安全的基础，提高用户对云平台的信任度是云计算技术向更深层次领域发展、全面普及和应用的关键。可信云计算技术是解决上述问题的一个有效手段。从保障云计算平台可信的角度出发，通过介绍可信虚拟化、可信云平台构建及可信虚拟机等相关技术的研究进展，分析并对比了典型方案的特点、适用范围及其在可信云计算领域的不同效用，讨论已有工作的局限性，进而指出未来发展趋势和后续研究方向。

关键词：云计算；可信计算；可信虚拟化；可信云平台；可信虚拟机

中图分类号：TP309

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019035

Survey on trusted cloud platform technology

HE Xinfeng[1,2,3], TIAN Junfeng[1,2,3], LIU Fanming[2,3]

1. School of Management, Hebei University, Baoding 071002, China
2. School of Cyber Security and Computer, Hebei University, Baoding 071002, China
3. Key Lab on High Trusted Information System of Hebei Province, Baoding 071002, China

Abstract: Information security technology confronts severe challenges because of the safety demands of cloud computing. The trustworthiness and self-safety of cloud computing platform are the foundation of cloud computing security. The confidence of cloud users is the key issue the deep development and popularization for cloud computing. The trusted cloud computing technology provides a feasible solution. From the standpoint of guaranteeing the trustworthiness of cloud computing platform, related research progresses on trusted virtualization, construction of trusted cloud platform and trusted virtual machine were introduced. Additionally, the characteristics, application scopes and effectiveness of typical schemes were analyzed and compared. Finally, current limitations and possible directions for future research were discussed.

Key words: cloud computing, trusted computing, trusted virtualization, trusted cloud platform, trusted virtual machine

1 引言

以虚拟化、资源租用、应用托管、服务外包等为典型应用的云计算（cloud computing），实现了人们长期以来的“把计算作为一种设施”的梦想[1]。当前，云计算发展面临许多关键性问题，其中的安全问题已成为制约云计算进一步发展的重要因素[2]。

一般认为，云计算环境自身的结构特点是造成安全问题的主要原因[3]。在云计算环境中，用户基本丧失了对私有信息和数据的控制能力，从而引起

收稿日期：2018−07−30；**修回日期**：2019−01−29

基金项目：河北省自然科学基金资助项目（No.F2016201064）；河北省自然科学基金重点资助项目（No.F2016201244）；河北省高等学校科学技术研究基金资助项目（No.ZD2015088）

Foundation Items: The Natural Science Foundation of Hebei Province (No.F2016201064), The Natural Science Foundation of Hebei Province - Key Program (No.F2016201244), The Natural Science Foundation of Hebei Institution (No.ZD2015088)

了一系列重要的安全挑战[4]，增强云计算平台自身的安全性是保证云计算安全的基础，提高用户对云计算平台的信任度是云计算技术向更深层次领域发展、全面普及和应用的关键。构建可信云计算平台是解决上述问题的一个有效手段。2017 年，中国工程院院士沈昌祥在《用可信计算构筑云计算安全》主旨报告中提出，要用可信计算构筑云计算安全，在云的基础上解决数据安全[5]。其他学者也从数据存储外包、计算外包、虚拟机外包等涉及云服务安全可信的领域开展了相关的研究工作[6]。

本文将从可信虚拟化、可信云平台构建和可信虚拟机等角度出发，综述近年来可信云计算技术的研究进展，具体分类如图 1 所示。通过介绍相关研究进展，分析并对比典型方案的特点和适用范围，讨论已有工作的局限性，进而指出未来发展趋势和后续研究方向。

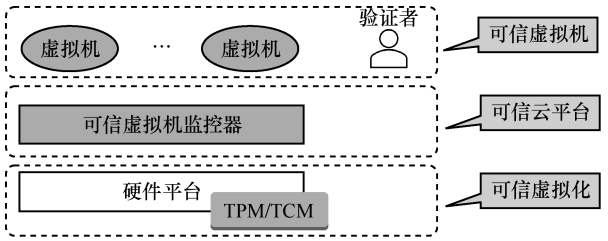


图 1　可信云计算研究分类

2　可信虚拟化

虚拟化是云计算的核心特征之一，通过虚拟化技术使 CPU、内存、硬盘等计算资源和存储资源得到合理共享和充分利用。将可信计算技术引入云计算，也需要进行虚拟化处理，以满足云计算的需求。可信计算组织（TCG, trusted computing group）虚拟化工作组（virtualized platform）提出了虚拟可信平台模块（vTPM, virtual trusted platform module）的概念[7-8]，为云计算环境提供可信功能。它通过模拟硬件 TPM（trusted platform module）的接口和功能，使每个虚拟机拥有自己独立的 vTPM，达到保护敏感信息、存储虚拟环境度量值、提供远程证明等目的，从而实现多个虚拟机 TPM 硬件资源的共享与复用。

TPM 的虚拟化主要有 TPM passthrough、基于函数库（如 libtpms）模拟以及 CUSE（character device in userspace）TPM 这 3 种实现方式，其中后 2 种都属于软件模拟 TPM 虚拟化方式[9]。3 种实现方式的各自特征如表 1 所示。

表 1　　TPM 的虚拟化方式

TPM 虚拟化方式	实现机制	并发访问支持	与物理 TPM 关系
TPM passthrough	I/O 虚拟化	单个虚拟机独占	直接访问
基于函数库模拟	函数库模拟，如 libtpms	多虚拟机并发	完全脱离
CUSE TPM	虚拟用户空间字符设备/dev/vTPM0	多虚拟机并发	完全脱离

由于 TPM passthrough 方式可实现虚拟机与 TPM 的直接绑定，具有较好的可信性，大量的研究者基于此方式开展可信云平台构建研究，详见 3.2 节内容。

我国在可信计算领域起步并不晚，水平也不低，成果可喜[10]，已经建立了完整的自主可控可信计算体系，以国产密码算法为基础提出了可信密码模块（TCM, trusted cryptography module）标准。文献[11]给出了基于可信根服务器的虚拟 TCM 密钥管理方案。在该方案中，所有的虚拟可信密码模块 vTCM 密钥均通过 vTCM 管理器调用物理可信密码模块 TCM 芯片来产生，保证了密钥产生的规范性。文献[12]提出了一种全新的虚拟可信根设计方案，该方案以模块化的结构对可信根进行重构，各个模块之间通过内部统一的消息格式来协调合作，为云环境提供安全可靠的计算保障。

为了解决原有 TPM 存在的安全问题，满足更多场景的应用，TCG 将可信平台规范族升级到 2.0 版本。结合 TPM 2.0 的新特性，文献[13]提出了一个 Ng-vTPM 框架，由物理 TPM 产生 vTPM 密钥提供安全存储属性，基于物理 TPM 背书平台种子与虚拟背书密钥的映射关系，提供虚拟机可信身份，将信任链由物理平台扩展到虚拟机平台，并提出使用基于平台配置寄存器策略的封装存储方法解决 vTPM 迁移后数据的可用性。

目前，可信虚拟化还面临功能缺失和性能受限这两方面的问题。从功能角度考虑，多数虚拟化方案通过软件来模拟 TPM 的功能，失去了可信计算技术使用硬件保护敏感信息的初衷。因此，可信计算技术原有的技术特征并不能完全体现在虚拟化后的方案中，如非易失存储、平台配置信息等。从性能角度考虑，当虚拟化方案采用 TPM passthrough 实现方式时，则某一时刻物理 TPM 只能被单个虚拟机独占，这将严重影响可用性，不适合在大规模的云平台使用。此外，云计算和虚拟化环境具有大

规模、分布式、动态、不确定性的特点，这就需要进行大量的、高效率的可信度量。受限于目前 TPM 的设计及实现方式，现有虚拟化方案面对大量的、高频率的可信度量时显得力不从心，无法满足云计算平台的全部可信度量需求。

为了更好地适应云计算平台的需求，根本的解决方法是增加可信芯片的运算能力和控制能力，更好地为云计算平台服务。国产可信计算标准创新性地提出了主动控制的可信平台控制模块（TPCM, trusted platform control module）概念[14]，使用对称密码与非对称密码相结合, 以 TPCM 为根进行主动控制和可信度量，提高了安全性和效率，改变了 TPM 模块作为被动设备的传统思路, 将可信平台模块设计为主动控制节点，实现了 TPCM 对整个平台的主动控制[15]。以 TPCM 为基础进行可信虚拟化设计，一方面可以利用 TPCM 主动的、绝对的控制能力，对云平台节点实施动态监控，保持其运行环境的可信性。一旦有恶意代码入侵而导致系统失控，TPCM 可以采取切断物理通道、关闭电源等绝对性保护措施保护数据及网络安全。另一方面，TPCM 不再从属于 CPU，可以进行独立的设计，具有比 TPM 更好的性能，可较好地解决功能缺失和性能受限的问题。TPCM 必将成为未来可信计算虚拟化技术的一个发展方向。但目前国产可信计算标准还处于发展的初期阶段，TPCM 普及程度较低，相关产品较少，还需要进一步加快产业化进程。

3 可信云平台构建

可信云平台通过可信计算技术为用户提供可信云服务，是可信云计算技术最直接的体现方式。目前，构造可信云平台的主要方案包括：1) 借助硬件隔离技术构造可信执行环境（TEE, trusted execution environment），如 Intel 的 SGX（software guard extension）、ARM 的 TrustZone 等，为虚拟机监控器添加安全隔离、可信验证等功能；2) 基于可信虚拟化（如 vTPM）技术构建可信云平台；3) 通过建立可信第三方，对云计算平台进行动态可信度量；4) 以可信安全芯片的密钥管理为基础，将终端密钥管理转化为云平台密钥管理，借此为虚拟机提供可信服务。此外，还出现了其他可信云平台构建方案。

3.1 基于 TEE 的可信云平台

TEE 技术主要通过硬件隔离技术保证代码的机密性和完整性，从而达到在不可信的环境中保证特定应用可信的目的。

早在 2003 年，Garfinkel 等[16]就提出了 Terra 模型，构建可信虚拟机监控器（TVMM, trusted virtual machine monitor），通过将虚拟机放置于 open box 和 closed box 的方式来实现安全隔离，但受限于当时硬件平台的性能，方案的优势不能充分发挥。为了更好地实现安全隔离，Intel 和 ARM 分别提出了基于处理器的安全隔离方案，为 TEE 的实现奠定了良好的基础。

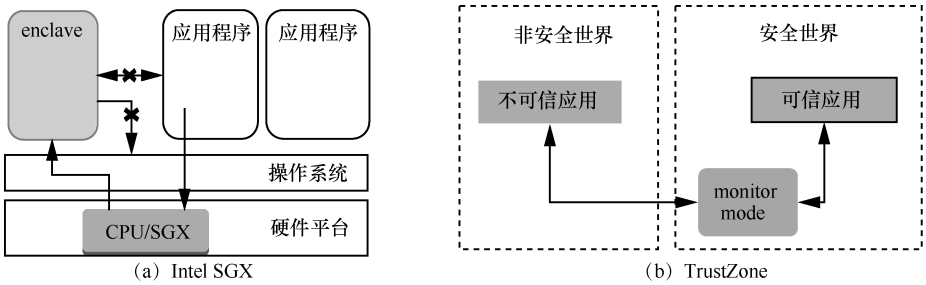
Intel SGX 技术首先应用于 Skylake 处理器，用于增强软件的安全性。这种方式将合法代码和数据封装在一个被称作 enclave 的容器中，保护其不受恶意软件的攻击，特权或者非特权的软件都无法访问 enclave，即使操作系统或者 VMM（hypervisor）也无法影响 enclave 里面的代码和数据。enclave 的安全边界只包含 CPU 和它自身。同时 SGX 还提供了对这些代码和数据的远程证明功能。

TrustZone 是 ARM 针对消费电子设备设计的一种硬件架构，目的是为消费电子产品构建一个安全框架来抵御各种可能的攻击。TrustZone 在概念上将 SoC（system on chip）的硬件和软件资源划分为安全世界（secure world）和非安全世界（normal world），所有需要保密的操作（如指纹识别、密码处理、数据加解密、安全认证等）在安全世界执行，其余操作（如用户操作系统、各种应用程序等）在非安全世界执行，安全世界和非安全世界通过一个名为 monitor mode 的模式进行转换。

Inter SGX 和 TrustZone 的基本体系如图 2 所示，这 2 种方式的联系与区别如表 2 所示。

基于 SGX 技术，Schuster 等[17]提出了 VC3 模型，保证在使用云平台进行 MapReduce 计算时，代码、数据以及运算结果的可信性。Jain 等[18]还提出了开源的 TEE 实验平台 OpenSGX，可实现 Intel SGX 的指令级模拟，为硬件安全隔离技术的应用、开发提供实验、测试环境。

在移动云计算领域，文献[19]利用 TrustZone 硬件隔离技术构建可信移动终端，保护云服务客户端及安全敏感操作在移动终端上的安全执行, 结合物理不可克隆函数技术，给出了移动终端密钥与敏感数据管理机制。Santos 等[20]利用 TrustZone 技术提出并实现了 TLR（trusted language runtime），用于构建与操作系统和其他应用隔离的可信组件，从



（a）Intel SGX　　（b）TrustZone

图 2　Intel SGX 和 TrustZone 的基本体系

表 2　　Intel SGX 和 TrustZone 的联系与区别

对比技术	信任根	隔离环境个数	动态可信度量	并发性	支持的功能
Intel SGX	CPU 和 enclave	多个	支持	多个 enclave 并发执行	安全隔离，远程证明
ARM TrustZone	硬件平台、trust OS	2 个	支持	串行	安全启动，安全隔离

而保证移动应用的机密性和完整性。

3.2　基于可信虚拟化的可信云平台

可信虚拟化的目标是为云计算环境提供可信支持，因此，基于 vTPM 构建可信云平台是此类研究的主要方向之一。文献[21]提出了一种基于信任扩展的可信虚拟执行环境的构建方法，实现 vTPM 与底层可信计算基的绑定，从而构建了可信虚拟执行环境。文献[22-23]通过 vTPM 扩展现有可信链，将可信传递到用户虚拟机内部，提出了一种动态的用户运行环境可信性验证机制，并将 vTPM 和可信审计技术结合起来，建立了用户可信运行环境的构建与审计机制。文献[24]提出的多租户可信计算环境模型（MTCEM, multi-tenancy trusted computing environment model）利用 TPM/vTPM 将云计算服务的安全职责进行分离，采用云提供商和用户协作的方式保证云节点平台的执行环境可信，云提供商负责基础设施的可信，用户负责虚拟机实例和应用程序的可信。文献[25]提出的 POSTER 利用基于 TPM/vTPM 的可信网络连接保护云服务端和云客户端之间的通信安全，从而为云计算提供端到端的可信保护。

在产业界，Intel 给出了基于 TPM/vTPM 的，以全面保护虚拟计算环境为目的的数据可信方案——可信执行技术（TXT, trusted execution technology）。TXT 通过硬件密钥和子系统双路控制电脑内部资源，并决定哪些程序、哪些用户允许访问或拒绝访问这些资源。TPM 与 DMA（direct memory access）页面保护共同构成了这项技术的主要内容。以 TXT 为基础，Intel 还给出了 trusted pool 和 trusted cloud 的概念，为以 Intel 处理器为核心的云计算节点提供可信服务，支持可信云平台的构建。

3.3　基于可信第三方的可信云平台

使用可信第三方（TTP, trusted third party）实现安全管理是简化管理过程的最佳手段，TTP 已经在大量的安全协议中有成熟的应用。结合 TTP 也可实现云计算平台的可信管理。使用 TTP 的主要思想是建立一个独立于云提供商的可信协调中心（TC, trusted coordinator），提供用户对云计算平台执行环境、虚拟机状态的可信状态监测和控制，如图 3 所示。

Santos 等[26]提出了可信云计算平台（TCCP, trusted cloud computing platform），该平台通过 TC 管理云中的所有可信节点，但当节点规模很大时，

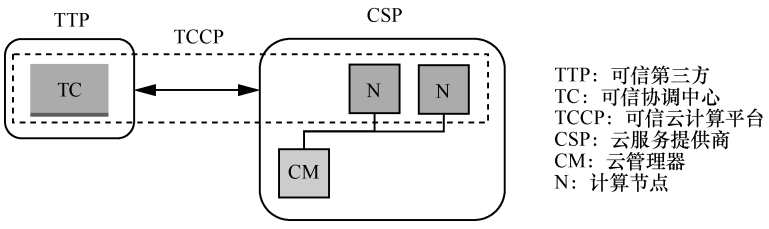


图 3　基于 TTP 的可信云平台架构

管理这些节点的时间开销过大。随后 Santos 等[27]对 TCCP 进行了改进，设计了 Excalibur 系统，该系统通过引入多个中心化的监视器来改进管理可信节点所造成的性能瓶颈。文献[28]针对可信云平台构建过程中可信节点动态管理存在的性能瓶颈问题，提出了基于 TPM 联盟的可信云平台体系结构及管理模型，引入了时间树的概念组织 TPM 联盟，利用 TPM 和认证加密技术解决数据在 TPM 联盟内节点间的可信传输问题。

3.4 其他方案及小结

此外，从其他角度实现可信云平台的构建方案也非常具有参考价值。针对 TPM 进行可信度量时的效率和多租户安全隔离问题，文献[29]提出的 cTPM 通过 TPM 和云平台共享一个云密钥来解决 TPM 资源受限的问题。文献[30]给出了一个高度自治的多租户网络安全框架 Jobber，用于适应云数据中心的动态特性和优化租户之间的通信。文献[31]对云租户隔离机制进行定义，并制定了云计算平台中域间信息流策略控制方式。文献[32]提出了基于可验证计算的可信云计算研究，成为实现可信云计算的一种建设性思路。

上述研究工作虽然以不同的方式研究了云计算平台的安全、可信问题，并给出了相应的解决方案，但大多方案集中在如何保障计算节点的可信性，忽略了云计算环境的典型特征，即高度资源共享和分布式管理。云平台作为管理各类 IT 资源的基础设施，需要实现计算节点、虚拟机、存储、网络等全面的可信方案，这就需要可信证据的传递与管理、跨主机/网络的可信度量、分布式可信协同机制等一系列技术的支持。单个计算节点可信并不等同于云平台可信，上述研究方案中使用的硬件隔离技术（如 SGX 等）和可信虚拟化技术（如 vTPM 等）都以保证节点内部可信为基础，缺乏可信证据跨节点传递和度量的机制，无法做到在云平台范围内可信状态的一致性与连续性。基于密钥共享类方案，如文献[29]，虽可实现云平台节点间的信任传递，但由于缺乏可信硬件的支持，难以实现真正意义上的可信云平台，因此，现有的研究工作还缺乏完善的解决方案。

4 可信虚拟机

可信计算主要解决计算终端可信问题，为此提出了诸如密钥管理、数据绑定、可信启动、身份认证、远程证明等一系列保证终端可信的概念。在云计算平台中，虚拟机是保证云服务可信的前提，保证其行为可预期至关重要，将可信计算用于计算终端的相关技术移植到虚拟机，来保障虚拟机的可信自然就成为可信云计算的一个重要研究方向。可信计算技术的引入可以增强云平台租户对虚拟机的信心，提高对云计算技术的信任程度。

4.1 基于虚拟化的安全监控

针对虚拟化安全监控技术的研究出现较早，其主要思想是利用虚拟机管理器隔离和保护特定的安全工具。从实现技术的角度来看，基于虚拟化安全监控的研究工作主要分为内部监控和外部监控这 2 种方式。内部监控是在虚拟机中加载内核模块来拦截目标虚拟机的内部事件，而内核模块的安全通过虚拟机管理器来进行保护；外部监控通过在虚拟机管理器中对虚拟机中事件进行拦截，从而在虚拟机外部进行检测[33]。与内部监控相比，外部监控在安全性和生存性方面具有一定的优势，不易被攻击者屏蔽。虚拟机自省（VMI, virtual machine introspection）[34]技术是外部监控中最为流行的一种，被广泛地研究与改进，其架构如图 4 所示。美国 Sandia 国家实验室的 Payne 等[35]开发了提供 VMI 功能的程序库 LibVMI，该程序库可对虚拟机的内存、硬件中断和 vCPU 的寄存器进行监控。VMI 利用一个隔离和安全的虚拟机监视其他的虚拟机，隔离主要依赖 VMM 来实现。由于 VMI 只能通过 VMM 获取虚拟机的原始数据，语义级别较低，而安全监控往往需要了解数据的高层语义信息，因此，如何跨越语义鸿沟是 VMI 的一个研究热点问题[36-39]。文献[40]首次提出了基于虚拟化安全监控的通用性问题，同时提出了一种基于驱动的通用监控系统——VMDriver 来实现细粒度监控，从而动态地屏蔽虚拟机中客户操作系统的差异，保证了监控系统的通用性。

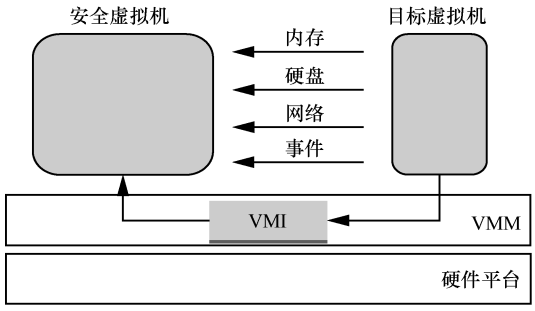


图 4 虚拟机自省技术架构

但基于虚拟化的安全监控技术并不能覆盖可信虚拟机的全部要求，如可信启动、数据平台绑定等，同时 VMI 默认 VMM 和 VMI 的代码是绝对可信的，但现实中这个假设未必成立。针对这个问题，文献[41]给出了一个 T-VMI 模型，该模型借助硬件隔离技术在云计算环境中实现虚拟机安全监控。此外，由于设计目标的不同，VMI 重点研究的是低级语义与高级语义之间的语义鸿沟问题，以此来判断虚拟机是否遭受恶意的外部攻击，但并不能保证虚拟机自身的动态可信。在现有的研究中，大量模型并没有引入可信计算技术，无法给出一个得到广泛认可的可信根，虚拟机的可信性也就无法保障。

4.2　虚拟机的可信启动

可信启动是可信计算技术中用于保证终端可信的技术之一，已经广泛应用于多种类型的操作系统，如用于 Linux 平台的 IMA（IBM integrity measurement）架构及 Windows8/Windows10 的可信启动技术。将上述技术移植到虚拟机，实现虚拟机的可信启动成为保证虚拟机可信的方案之一。但虚拟机与计算终端有着明显的区别，因此还需要对可信启动方案进行适当调整。

文献[42]提出了一种解决在云平台基础设施服务策略下虚拟机的安全存储和可信启动方案 SSTL。根据 TPM 的一些核心功能，分别从 VM 镜像加解密、VM 宿主平台信息的远程证明和 VM 度量机制来保证 VM 存储安全、运行环境安全以及可信启动。利用可信技术中的封装、绑定等技术，文献[43]提出一个用于保证虚拟机实例可信启动的协议，为公有云用户虚拟机可信度量提供支持。

目前，专门针对虚拟机可信启动的技术研究较少，虚拟机的可信启动涉及虚拟镜像可信、云存储可信、节点环境可信、同驻虚拟机可信[44-45]等一系列问题。同时，虚拟机可信启动又是虚拟机可信的前提条件，未来的发展方向必然是与新一代的可信计算和虚拟化技术紧密结合，共同构筑虚拟机可信的第一道防线。

4.3　虚拟机的身份认证与远程证明

IMA 对计算终端的身份认证与远程证明也进行了相关的讨论，并提出了 2 种方案。一种方案是借助隐私签证机构 PCA（privacy CA），通过 PCA 对 TPM 身份验证、颁发证书 AIK（attestation identity key），并且对网内的 TPM 密钥管理分发、注销等；另一种方案称为直接匿名认证（DAA, direct anonymous attestation），根据零知识证明技术进行 TPM 身份的认证[46]。针对上述方案存在的计算开销大和无法满足跨域匿名认证需求等不足，还出现了一些改进方案[47-48]。

虚拟机托管在远程的云计算平台，租户无法对其进行直接控制，其运行可信状态的获取只能通过间接和远程的方式实现，对其身份认证和远程证明的需求比计算终端更为迫切。此外，虚拟机动态特性表现明显，其身份认证与远程证明必然也是动态进行的。而传统的可信计算技术往往采用 AIK、PCR 等静态内容作为认证的依据，与虚拟机的特征不符，一些研究工作针对传统方案进行了改进。

文献[49]提出了一种虚拟机身份证明方案，在保障原有认证和信任关系的情况下，实现了身份证明过程中对身份权威信息的隐藏，避免了上述组织结构、位置等信息的暴露，支持云环境结构透明、位置无关的特点。为了解决目前云环境下用户与云端之间进行身份认证时所存在的安全问题和不足，文献[50]将 PTPM（portable TPM）和无证书公钥密码体制应用到云环境中，提出了一种实现用户与云端之间双向身份认证的方案，确保了终端平台的安全可信和云端与用户之间认证结果的真实正确。

目前关于远程证明的研究主要包括基于实体标识的二进制证明和基于属性的远程证明[51-52]。其中，二进制远程证明方案通过实体对象散列值的完整性验证，得出终端是否可信的结论；而在云计算环境下，所有实体均被虚拟化、动态化，使用散列值已经难以描述 VM 的可信状态。此外，二进制远程证明只能验证 VM 启动等特定时刻的可信状态，而 VM 是动态的，状态随时会发生迁移等影响其可信性的操作，需要进行动态远程证明，二进制证明很难做到这一点。因此，已经有部分研究工作探讨如何在云环境下使用属性证明的方式实现虚拟机的远程证明。

文献[53]利用基于远程属性证明技术，监测和阻止针对云基础设施的安全攻击，从而保障租户的安全。文献[54]提出并设计了云安全监控系统 CloudPass，利用 TPM 和属性证明实现系统完整性和身份认证的目的。

目前的虚拟机身份认证与远程证明方案仍存在功能单一、可信属性缺乏规范性等不足，大量方案仅集中在解决虚拟机安全监控、匿名等部分问题，不能对云平台中的虚拟机实现实时、动态的身份认证和远程证明。基于属性的身份认证和远程证

明依然是未来研究工作的热点，但需对虚拟机实例在整个生命周期内的可信属性进行规范化处理，提出了对可信属性的形式化证明方法，进一步给出了虚拟机可信的理论依据。

4.4 虚拟机的可信迁移

虚拟机与计算终端存在着很多不同之处，使可信计算技术无法全面覆盖虚拟机可信的全部安全需求。虚拟机管理涉及虚拟机的生成、分配、回收、迁移等一系列问题[55]。保证虚拟机整个生命周期内的安全是实现云平台可信的基础，尤其是当虚拟机发生迁移后，如何确保目标平台的可信性和虚拟机可信状态的一致性是虚拟机整个生命周期安全管理需要解决的重点问题，也是难点问题。而传统的可信计算技术中并没有针对该问题的解决方案，导致虚拟机安全管理的功能缺失。虚拟机的可信迁移给上述问题的解决提供了一个可行方案。

虚拟机的可信迁移是指以现有可信计算技术为基础，保证虚拟机从云计算平台原计算节点迁移到目标计算节点后，仍可保持其可信状态的一致性和连续性，从而实现虚拟机生命周期内的可信度量。这里的可信状态主要指与虚拟机绑定的各类密钥（包括 AIK、存储根密钥等）、软硬件平台配置信息（PCR 内容）、隐私数据及其他相关数据。

虚拟机迁移是云计算中的核心技术之一，具有负载均衡、解除硬件依赖、高效利用资源等优点，但也会将虚拟机信息和用户信息暴露在网络通信中，成为云计算脆弱性的源头之一。虚拟机迁移过程除了会受到传统的网络攻击外，还有可能导致 co-residence 攻击的出现。co-residence 攻击是针对云平台的一种新型攻击手段，基本思想是利用虚拟机之间共享的硬件计算资源，进行旁路（side channel）攻击，获取敏感信息。传统的网络安全措施对其无法防范。文献[56]给出了 co-residence 攻击产生的原因，并实现了名为 HomeAlone 的系统工具，用于检测用户虚拟机是否存在 co-residence 攻击。文献[57]给出了一种虚拟机分配策略，该策略降低产生 co-residence 攻击的可能性。文献[58]则在 Amazon EC2（elastic compute cloud）公有云上进行了测试，说明了 co-residence 攻击存在的普遍性。文献[59]深入分析了跨虚拟机 cache 侧信道攻击的机理和实现方式，对跨虚拟机 cache 侧信道攻击技术的研究现状与进展进行总结。

依据可信云平台的实现机制不同，目前虚拟机可信迁移方案也分为多种类型，如基于 vTPM 的虚拟机可信迁移、基于密钥管理的虚拟机可信迁移等。文献[60]提出了一种适用于私有云环境的虚拟机安全迁移协议，该协议基于 vTPM 构建分级云密钥来保证虚拟机在迁移前后的机密性和完整性。文献[61]给出了一个 VM-vTPM 虚拟机可信迁移协议，并对协议的安全性和性能进行了定量分析。在公有云领域，文献[62]给出了虚拟机从一个云服务提供商（CSP, cloud service provider）迁移到其他 CSP 的安全机制。文献[63]给出了在异构的云环境中，如何使用可信计算技术来增强云平台的可信性，特别是虚拟机迁移时的可信性。文献[64]结合可信计算中的密钥管理技术，提出了虚拟机可信证据的概念，并给出了一种应用于 IaaS 平台的可信虚拟机迁移协议，确保虚拟机在迁移前后的可信状态的一致性和连续性，为 IaaS 平台提供虚拟机的可信迁移支持。文献[65]分析了虚拟机动态迁移时的内存泄漏安全隐患，结合 KVM（kernel-based virtual machine）虚拟化技术原理、通信机制、迁移机制，设计并提出一种基于混合随机变换编码方式的安全防护模型，保证虚拟机动态迁移时的数据安全。文献[66]针对可信虚拟机的迁移缺乏统一的安全模型及测试方法问题，提出了一种可信虚拟机迁移框架，对可信迁移的过程进行了抽象，并使用标号迁移系统 LTS 进行了形式化的描述。

虚拟机的可信迁移是保证虚拟机在整个生命周期内行为可控、可预期的基础，对整个云平台的可信性起着至关重要的作用，是保证虚拟机可信的重要一环。虚拟机有着比物理终端更为动态化的行为，对其进行可信度量和评价也是一个较为复杂的问题。现有研究工作分别从虚拟机可信启动、身份认证与远程证明及可信迁移等多方面进行了讨论，但尚无完整机制能够全面保障虚拟机可信。结合可信云平台构建方案，开展统一的虚拟机可信度量、评价机制研究，保证虚拟机在整个生命周期内行为的可控、可预期，必将是未来研究工作的重点。

5 未来研究展望

本文主要围绕可信云计算的最新研究内容展开综述，介绍了近年来具有代表性的可信虚拟化及可信云平台构建技术。通过分析可以看出，现有可信云计算领域仍然存在大量尚未解决的问题，未来的科研工作可以更多地关注以下几点。

1) 适用于云计算的可信虚拟化方案。前述内容已说明，现有的可信虚拟化方案存在可信功能缺失和性能受限两方面的问题，不能满足云计算平台的可信度量的全部要求。要实现该问题的突破，需要对现有可信计算技术的体系做较大规模的调整，这有可能成为可信云计算技术，甚至是可信计算技术未来研究的重点之一。

2) 可信云平台的协同工作问题。现有的可信云平台构建方案重点在于对计算节点可信度量，而针对节点间可信协同问题的研究相对较少。但云计算平台是一个典型的分布式系统，所有机制均建立在协同工作的基础上，研究适用于云计算平台的分布式可信度量方案是未来可信云平台的研究方向之一。

3) 提出更为完善的虚拟机可信度量机制，支持虚拟机启动、远程证明、动态迁移等整个生命周期的可信状态一致性、连续性和完整性，形成一套完整的可信云平台构建解决方案。

4) 建立自主可控可信云平台构建标准。2016 年，微软公布所有 Win10 新设备必须默认支持 TPM 2.0 规范，并且 TPM 芯片必须默认激活状态，这说明可信计算技术在计算终端领域已逐步进入推广阶段。与国外普遍采用的 TCG 系列标准不同，我国已经初步建立了自主可控的可信计算标准，要占领信息安全高地，必须也要建立自己的可信云平台构建标准，从云计算节点可信、虚拟机可信、传输可信、用户行为可信等多角度保障云基础设施的自主、安全、可控，掌握芯片、云操作系统、网络服务器等软硬件的核心技术，扼守我国关键信息基础设施的安全大门。

6　结束语

可信云计算技术将可信计算理论及技术应用于云平台的构建，以保证云平台的可信性，增加用户对云计算技术的信任度。在可信云计算领域，国内外已取得较好的研究成果，但是仍有许多遗留问题尚待探讨，本文重点介绍了当前可信云计算技术中可信计算、云计算相互融合、相互支持的方式，分别围绕可信虚拟化、可信云平台构建和可信虚拟机 3 个研究热点问题展开综述，以期为可信云计算技术的未来研究做出一些有益的探索。

参考文献：

[1] 林闯, 苏文博, 孟坤,等. 云计算安全:架构、机制与模型评价[J]. 计算机学报, 2013,36(9):1765-1784.
LIN C, SU W B, MENG K, et al. Cloud computing security: architecture, mechanism and modeling[J]. Chinese Journal of Computers, 2013, 36(9): 1765-1784.

[2] 冯登国, 张敏, 张妍,等. 云计算安全研究[J]. 软件学报, 2011, 22(1):71-83.
FENG D G, ZHANG M, ZHANG Y, et al. Study on cloud computing security[J]. Journal of Software, 2011,22(1): 71-83.

[3] ALANI M M. Securing the cloud: threats, attacks and mitigation techniques[J]. Journal of Advanced Computer Science & Technology, 2014, 3(2):202.

[4] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J].软件学报,2016, 27(6):1328-1348.
ZHANG Y Q, WANG X F, LIU X F, et al. Survey on cloud computing security[J]. Journal of Software, 2016, 27(6):1328-1348.

[5] 沈昌祥. 用可信计算构筑云计算安全[J]. 中国经贸导刊, 2017(16):56-57.
SHENG C X. Constructing cloud security with trusted computing[J].China Economic & Trade Herald, 2017(16):56-57.

[6] 丁滟, 王怀民, 史佩昌,等. 可信云服务[J]. 计算机学报, 2015, 38(1):133-149.
DING Y, WANG H M, SHI P C, et al. Trusted cloud service[J]. Chinese Journal of Computers, 2015, 38(1):133-149.

[7] BERGER S, CERES R, GOLDMAN K A, et al. vTPM: virtualizing the trusted platform module[C]// Conference on Usenix Security Symposium. USENIX Association, 2006:21.

[8] STEFAN B, RAMÓN C, KENNETH A G, et al. vTPM: virtualizing the trusted platform module[J]. Usenix Security, 2007, 15:305-320.

[9] BERGER S, GOLDMAN K, PENDARAKIS D, et al. Scalable attestation: a step toward secure and trusted clouds[C]// IEEE International Conference on Cloud Engineering. IEEE, 2015:185-194.

[10] 沈昌祥, 张焕国, 王怀民,等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010(2):139-166.
SHEN C X, ZHANG H G, WANG H M,et al. The research & development of trusted computing[J]. Science China Information Sciences, 2010(2):139-166.

[11] 王冠, 袁华浩. 基于可信根服务器的虚拟 TCM 密钥管理功能研究[J]. 信息网络安全, 2016(4):17-22.
WANG G, YUAN H H. Research of virtual trusted cryptography module's secret key management based on the trusted root server[J]. Netinfo Security, 2016(4):17-22.

[12] 张建标, 赵子枭, 胡俊,等. 云环境下可重构虚拟可信根的设计框架[J]. 信息网络安全, 2018(1):1-8.
ZHANG J B, ZHAO Z X, HU J, et al. The design framework of reconfigurable virtual root of trust in cloud environment[J]. Netinfo Security, 2018(1):1-8.

[13] 杨永娇, 严飞, 毛军鹏,等. Ng-vTPM:新一代TPM虚拟化框架设计[J]. 武汉大学学报(理学版), 2015, 61(2):103-111.
YANG Y J, YAN F, MAO J P, et al. Ng-vTPM: a next generation virtualized TPM architecture[J]. Journal of Wuhan University(Natural Science Edition), 2015, 61(2):103-111.

[14] 沈昌祥,公备. 基于国产密码体系的可信计算体系框架[J]. 密码学报, 2015(5): 381-389.
SHEN C X, GONG B. The innovation of trusted computing based on the domestic cryptography. Journal of Cryptologic Research, 2015(5): 381-389.

[15] 黄坚会, 沈昌祥, 谢文录. TPCM 三阶三路安全可信平台防护架构[J]. 武汉大学学报(理学版), 2018(2):109-114.
HUANG J H, SHEN C X, XIE W L. The TPCM 3P3C defense archi-

tecture of safety and trusted platform[J]. Journal of Wuhan University(Natural Science Edition), 2018(2):109-114.

[16] GARFINKEL T, PFAFF B, CHOW J, et al. Terra:a virtual machine-based platform for trusted computing[C]//ACM Symposium on Operating Systems Principles. 2003:193-206.

[17] SCHUSTER F, COSTA M, FOURNET C, et al. VC3: trustworthy data analytics in the cloud using SGX[C]// IEEE Symposium on Security and Privacy. 2015:38-54.

[18] JAIN P, DESAI S, KIM S, et al. OpenSGX: an open platform for SGX research[C]//The Network and Distributed System Security Symposium. 2016.

[19] 杨波, 冯登国, 秦宇,等. 基于 TrustZone 的可信移动终端云服务安全接入方案[J]. 软件学报, 2016, 27(6):1366-1383.
YANG B, FENG D G, QIN Y, et al. Secure access scheme of cloud services for trusted mobile terminals using TrustZone[J]. Journal of Software, 2016, 27(6):1366-1383.

[20] SANTOS N. Using ARM TrustZone to build a trusted language runtime for mobile applications[C]//International Conference on Arohitectural Support for Programming Languages & Operating Systems. 2016: 67-80.

[21] 王丽娜, 高汉军, 余荣威,等. 基于信任扩展的可信虚拟执行环境构建方法研究[J]. 通信学报, 2011, 32(9):1-8.
WANG L N, GAO H J, YU R W, et al. Research of constructing trusted virtual execution environment based on trust extension[J]. Journal on Communications, 2011, 32(9):1-8.

[22] 刘川意, 林杰, 唐博. 面向云计算模式的运行环境可信性动态验证机制[J]. 软件学报, 2013, 24(1): 1240-1252.
LIU C Y, LIN J, TANG B. A dynamic trustworthiness verification mechanism for trusted cloud execution environment. [J]. Journal of Software, 2013, 24(1):1240-1252 .

[23] 刘川意, 王国峰, 林杰,等. 可信的云计算运行环境构建和审计[J]. 计算机学报, 2016, 39(2):339-350.
LIU C Y, WANG G F, LIN J, et al. Practical construction and audit for trusted cloud execution environment[J].Chinese Journal of Computers, 2016, 39(2):339-350.

[24] LI X Y, ZHOU L T, SHI Y, et al. A trusted computing environment model in cloud architecture[C]//International Conference on Machine Learning and Cybernetics. 2010:2843-2848.

[25] WANG J, ZHAO B, ZHANG H, et al. POSTER: an E2E trusted cloud infrastructure[C]//The ACM SIGSAC Conference on Computer and Communications Security. 2014:1517-1519.

[26] SANTOS N, GUMMADI K P, RODRIGUES R. Towards trusted cloud computing[C]// Conference on Hot Topics in Cloud Computing. USENIX Association, 2009:3.

[27] SANTOS N, RODRIGUES R, GUMMADI K P, et al. Policy-sealed data: a new abstraction for building trusted cloud services[C]// USENIX Conference on Security Symposium, 2012: 1-14.

[28] 田俊峰, 常方舒. 基于 TPM 联盟的可信云平台管理模型[J]. 通信学报, 2016, 37(2):1-10.
TIAN J F, CHANG F S. Trusted cloud platform management model based on TPM alliance[J]. Journal on Communications, 2016, 37(2): 1-10.

[29] CHEN C, RAJ H, SAROIU S, et al. cTPM: a cloud TPM for cross-device trusted applications[C]//The USENIX Conference on Networked Systems Design and Implementation. 2014: 187-201.

[30] SAYLER A, KELLER E, GRUNWALD D. Jobber: automating inter-tenant trust in the cloud[C//Workshop on Hot Topics in Cloud Computing. 2013: 1-6.

[31] 石勇,郭煜,刘吉强,等.一种透明的可信云租户隔离机制研究[J].软件学报,2016,27(6):1538-1548.
SHI Y, GUO Y, LIU J Q, et al. Trusted cloud tenant separation mechanism supporting transparency[J]. Journal of Software, 2016, 27(6): 1538-1548.

[32] 王佳慧, 刘川意, 王国峰,等. 基于可验证计算的可信云计算研究[J]. 计算机学报, 2016, 39(2):286-304.
WANG J H, LIU C Y, WANG G F, et al. Review of trusted cloud computing based on proof-based verifiable computation[J].Chinese Journal of Computers, 2016, 39(2):286-304.

[33] 项国富, 金海, 邹德清,等. 基于虚拟化的安全监控[J]. 软件学报, 2012, 23(8):2173-2187.
XIANG G F, JIN H, ZOU D Q, et al. Virtualization-based security monitoring[J].Journal of Software, 2012, 23(8): 2173-2187.

[34] GARFINKEL T. A virtual machine introspection based architecture for intrusion detection[J]. Proc.network & Distributed Systems Security Symp, 2003:191-206.

[35] PAYNE B D. Simplifying virtual machine introspection using LibVMI[J]. Office of Scientific & Technical Information Technical Reports, 2012: 1-20.

[36] 李保珲, 徐克付, 张鹏, 等. 虚拟机自省技术研究与应用进展[J].软件学报, 2016, 27(6):1384-1401.
LI B H, XU K F, ZHANG P, et al. Research and application progress of virtual machine introspection technology[J].Journal of Software, 2016,27(6):1384-1401.

[37] SCHIFFMAN J, VIJAYAKUMAR H, JAEGER T. Verifying system integrity by proxy[M]. Berlin: Springer, 2012:179-200.

[38] ZHANG T, LEE R B. CloudMonatt: an architecture for security health monitoring and attestation of virtual machines in cloud computing[C]// International Symposium on Computer Architecture. 2015:362-374.

[39] ZHANG T, LEE R B. Monitoring and attestation of virtual machine security health in cloud computing[J]. IEEE Micro, 2016, 36(5):28-37.

[40] XIANG G, JIN H, ZOU D, et al. VMDriver: a driver-based monitoring mechanism for virtualization[C]// Reliable Distributed Systems. 2010:72-81.

[41] JIA L, ZHU M, TU B. T-VMI: trusted virtual machine introspection in cloud environments[C]// International Symposium on Cluster, Cloud and Grid Computing. 2017:478-487.

[42] 王庆飞, 严飞, 王鹃,等. IaaS 下虚拟机的安全存储和可信启动[J]. 武汉大学学报(理学版), 2014, 60(3):231-236.
WANG Q F, YAN F, WANG J, et al. Secure storage and trusted launch of virtual machine in IaaS[J]. Journal of Wuhan University(Natural Science Edition), 2014, 60(3):231-236.

[43] PALADI N, GEHRMANN C, ASLAM M, et al. Trusted launch of virtual machine instances in public IaaS environments[M]. Berlin: Springer. 2013.

[44] ZHANG Y, JUELS A, OPREA A, et al. HomeAlone: co-residency detection in the cloud via side-channel analysis[C]// Security and Privacy. 2011:313-328.

[45] EZHILCHELVAN P, MITRANI I. Evaluating the probability of malicious co-residency in public clouds[J]. IEEE Transactions on Cloud Computing, 2017, 5(3):420-427.

[46] SMYTH B, RYAN M, CHEN L. Direct anonymous attestation (DAA): ensuring privacy with corrupt administrators[C]// European Conference on Security and Privacy in Ad-Hoc and Sensor Networks. 2007:218-231.

[47] 杨力, 张俊伟, 马建峰, 等. 改进的移动计算平台直接匿名证明方案[J]. 通信学报, 2013, 34(6): 69-75.
YANG L, ZHANG J W, MA J F, et al. Improved direct anonymous attestation scheme for mobile computing platform[J]. Journal on Communications, 2013, 34(6):69-75.

[48] 周彦伟, 杨波, 吴振强,等. 基于身份的跨域直接匿名认证机制[J]. 中国科学:信息科学, 2014, 44(9):1102-1120.
ZHOU Y W, YANG B, WU Z Q, et al. Direct anonymous authentication scheme in cross-domain based on identity[J]. Science China Information Sciences, 2014, 44(9): 1102-1120.

[49] 张严, 冯登国, 于爱民. 云计算环境虚拟机匿名身份证明方案[J]. 软件学报, 2013, 24(12):2897-2908.
ZHANG Y, FENG D G, YU A M. Virtual machine anonymous attestation in cloud computing[J]. Journal of Software, 2013, 24(12): 2897-2908.

[50] 王中华, 韩臻, 刘吉强,等. 云环境下基于 PTPM 和无证书公钥的身份认证方案[J]. 软件学报, 2016, 27 (6):1523-1537.
WANG Z H, HAN Z, LIU J Q, et al. ID authentication scheme based on PTPM and certificateless public key cryptography in cloud environment[J]. Journal of Software, 2016, 27(6): 1523-1537.

[51] 于爱民, 冯登国, 汪丹. 基于属性的远程证明模型[J]. 通信学报, 2010, 31(8):1-8.
YU A M, FENG D G, WANG D. Property-based remote attestation model[J].Journal on Communications, 2010, 31(8):1-8.

[52] 冯登国, 秦宇. 一种基于 TCM 的属性证明协议[J]. 中国科学:信息科学, 2010, 40(2):189-199.
FENG D G, QIN Y. A property attestation protocol based on TCM[J].Science China Information Sciences, 2010, 40(2):189-199.

[53] NING Z H, JIANG W, ZHAN J, et al. Property-based anonymous attestation in trusted cloud computing[J]. Journal of Electrical & Computer Engineering, 2014(17):1-7.

[54] AWAD A, KADRY S, LEE B, et al. Property based attestation for a secure cloud monitoring system[C]//IEEE/ACM International Conference on Utility and Cloud Computing. 2014: 934-940.

[55] AHMAD R W, GANI A, HAMID S H A, et al. A survey on virtual machine migration and server consolidation frameworks for cloud data centers[J]. Journal of Network & Computer Applications, 2015, 52(C): 11-25.

[56] ZHANG Y, JUELS A, OPREA A, et al. HomeAlone: co-residency detection in the cloud via side-channel analysis[C]//IEEE Symposium on Security and Privacy. 2011: 313-328.

[57] HAN Y, CHAN J, ALPCAN T, et al. Using virtual machine allocation policies to defend against co-resident attacks in cloud computing[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(1): 95-108.

[58] XU Z, WANG H, WU Z. A measurement study on co-residence threat inside the cloud[C]//The USENIX Conference on Security Symposium. 2015: 1-24.

[59] 梁鑫, 桂小林, 戴慧珺, 等. 云环境中跨虚拟机的 cache 侧信道攻击技术研究[J]. 计算机学报, 2017, 40(2):317-336.
LIANG X, GUI X L, DAI H J, et al. Cross-VM cache side channel attacks in cloud: a survey[J]. Chinese Journal of Computers, 2017, 40(2): 317-336.

[60] DANEV B, MASTI R J, KARAME G O, et al. Enabling secure VM-vTPM migration in private clouds[C]//The Annual Computer Security Applications Conference. 2011: 187-196.

[61] HONG Z, WANG J, ZHANG H G, et al. A trusted VM-vTPM live migration protocol in clouds[J]. Proceedings of International Workshop on Cloud Computing & Information Security, 2013, 52(1391): 299-302.

[62] ASLAM M, GEHRMANN C, BJORKMAN M. Security and trust preserving VM migrations in public clouds[C]// The IEEE International Conference on Trust, Security and Privacy in Computing and Communications.2012:869-876.

[63] CELESTI A, SALICI A, VILLARI M, et al. A remote attestation approach for a secure virtual machine migration in federated cloud environments[C]//IEEE Symposium on Network Cloud Computing and Applications. 2011:99-106.

[64] HE X, TIAN J. A trusted VM live migration protocol in IaaS[C]//Trusted Computing and Information Security. 2017: 41-52.

[65] 范伟, 孔斌, 张珠君, 等. KVM 虚拟化动态迁移技术的安全防护模型[J]. 软件学报, 2016,27(6):1402-1416.
FAN W, KONG B, ZHANG Z J, et al. Security protection model on live migration for KVM virtualization[J]. Journal of Software, 2016, 27(6):1402-1416.

[66] 石源, 张焕国, 吴福生. 一种可信虚拟机迁移模型构建方法[J]. 计算机研究与发展, 2017, 54(10):2284-2295.
SHI Y, ZHANG H G, WU F S. A method of constructing the model of trusted virtual machine migration[J]. Journal of Computer Research and Development, 2017, 54(10):2284-2295.

[作者简介]

何欣枫（1976− ），男，天津人，河北大学博士生，主要研究方向为云计算安全、可信计算等。

田俊峰（1965− ），男，河北保定人，博士，河北大学教授、博士生导师，主要研究方向为信息安全、分布式计算等。

刘凡鸣（1990− ），女，河北保定人，河北大学实验师，主要研究方向为大数据处理、云计算安全等。