可信云计算研究综述

张立强[1]，　吕建荣[1]，　严　飞[1]，　熊云飞[2]

(1. 武汉大学 国家网络安全学院 空天信息安全与可信计算教育部重点实验室　湖北 武汉 430072；
2. 烽火技术服务有限公司　湖北 武汉 430074)

摘要：云计算具有高性能、服务化、弹性伸缩、环境友好等优点，已经成为广泛采用的新型 IT 基础设施。资源外包与资源租赁的服务化本质，导致安全与隐私需求尤为突出，传统安全技术方案无法有效满足云计算的安全需求。为此，近年来学术界和工业界实现了一系列的安全改进和创新，试图用自底向上的思路解决云计算中的各类安全问题，构建可信云体系架构，以期实现云计算的安全可信。本文围绕云计算环境面临的安全威胁展开讨论，给出了当前主流的可信云计算实现思路与关键技术，讨论了相关工作的优势与不足，并对可信云计算的发展方向进行了探讨。

关键词：云计算；可信计算；安全威胁；可信云计算

中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1671-6841(2022)04-0001-11

DOI：10.13705/j.issn.1671-6841.2021487

Research on Trusted Cloud Computing Technologies

ZHANG Liqiang[1], LYU Jianrong[1], YAN Fei[1], XIONG Yunfei[2]

(1. *Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072, *China*;
2. *Fiberhome Technical Services Co., Ltd., Wuhan* 430074, *China*)

Abstract: With the advantages of high performance, servitization, elastic scale and environmental-friendliness, as a new IT infrastructure, cloud computing has been widely used. Because of its feature of resource outsourcing and resource renting, security and privacy requirements were of great importance. Traditional security technologies were unable to meet the requirements of security in cloud computing. So in recent years, vast security improvements and innovations were proposed in academia and industry. These schemes were used to solve various security problems in cloud computing bottom-up, and built a trusted cloud system architecture in order to achieve a secure and reliable cloud computing. Based on the security threats to cloud computing, the implementations and key technologies of trusted cloud computing were discussed. The advantages and drawbacks of the related works were summarized, and the developing directions of trusted cloud computing were discussed.

Key words: cloud computing; trusted computing; security threat; trusted cloud computing

0　引言

随着云计算的广泛使用，云计算技术本身的发展速度与相应的安全技术发展速度之间的差距逐渐增大，云安全问题日益凸显。McAfee 2017 云安全研究报告显示，有 23% 的企业完全信任公有云，而在 2016 年只有 13%[1]。2020 年，我国使用公有云的

收稿日期：2021-11-13
基金项目：国家自然科学基金项目(61272452,61872430)；湖北省重点研发计划项目(2020BAA001,2021BAA027)；苏州市前瞻性应用研究项目(SYG201845)。
第一作者：张立强(1979—)，男，副教授，主要从事可信计算与系统安全测评研究，E-mail：zhanglq@whu.edu.cn。
通信作者：严飞(1980—)，男，副教授，主要从事系统安全与可信计算研究，E-mail：yanfei@whu.edu.cn。

企业中,有6.3%曾遭遇到恶意木马攻击,在发现的木马中有27%未及时处理,公有云主机远程登录窗口被爆破次数超2.5亿次[2]。为了解决云计算所面临的日益严重的安全威胁,学术界和工业界提出了一系列保护云计算安全的解决方案。例如,为了解决云计算数据安全和内容隐私问题,相关学者提出了基于身份的代理重加密方案[3]、基于密钥的属性加密算法[4]等;为了抵抗针对云计算本身可用性的安全威胁(如拒绝服务攻击、僵尸网络攻击),相关学者提出了基于过滤的抗拒绝服务攻击技术[5]、云虚拟机的数据包自动过滤机制[6]等。这些基于加密、流量监测以及软件测试的安全防护方案能够解决一部分安全威胁。然而,相关工作仍然存在以下四个方面的不足。

1)这些防护方案仅能解决云计算某一方面的安全问题,如数据安全或应用安全,难以从整体上消除云计算所面临的安全威胁。

2)这些防护方案大部分仅能对已知的安全威胁做到有效防御,遇到未知的安全威胁时,已有的防护方案往往收效甚微。

3)基于软件检测的防护方案需要由云计算平台或云服务提供商对软件进行检测和评估,而实现这类防护方案的前提是云计算平台和云服务提供商具有很高的软件漏洞检测水平以及恶意软件检测水平,而这一点在实际的商业云环境中往往难以达到。

4)上述方案实现的前提是云服务提供商本身应当是良性而非恶意的,即云计算平台不会窃取用户隐私或欺骗用户,为用户提供恶意的云服务,而这一点在实际的生产环境中也是很难达到的。

为了从根本上解决云计算所面临的安全威胁,学术界结合可信计算技术与云计算技术,提出了可信云计算的概念[7],即从云计算的底层开始确保云计算基础设施的安全性,一级度量一级,一级信任一级,最终确保云计算从IaaS层到SaaS层的整体安全。本文将从云计算所面临的安全威胁以及可信云的发展入手,分析可信计算技术在确保云计算安全性中的作用,并对现有的可信云计算技术进行分析与总结,最后分析可信云计算所面临的挑战以及可能的解决方案。

1 云计算环境面临的安全威胁

云计算综合利用分布式计算、虚拟化、服务外包等技术,在获取诸多优势的同时,也在无形之中拓展了攻击平面。由于云计算环境基于虚拟化构建,因此在一个物理机上通常存在属于不同用户的云主机,这一特性使得云计算环境不仅需要考虑传统计算环境所面对的安全威胁,还需要考虑不可信的管理员以及恶意的云用户所带来的安全威胁。同时,由于云计算环境特有的物理环境以及网络拓扑结构,针对传统安全威胁的解决方案在云计算环境下并不适用。因此,云计算安全解决方案的关键是针对传统安全威胁和云环境特有的安全威胁来构建适用于云计算环境的解决方案。云计算面临的安全威胁如表1所示。

表1 云计算面临的安全威胁

Table 1 Security threats to cloud computing

威胁层次	威胁类型	威胁示例
IaaS	外部威胁	SQL注入、DDoS、平台渗透
	内部威胁	虚假服务、资源窃取、共存攻击
PaaS	破坏机密性	管理者窃取数据、侧信道攻击
	破坏可用性	DoS攻击、资源抢占攻击
SaaS	破坏机密性	管理者窃取用户隐私
	破坏可用性	恶意的SaaS提供商破坏用户终端,提供虚假业务

1.1 针对IaaS层的安全威胁

云计算在IaaS层所面临的安全威胁大致可分为传统安全威胁以及云计算环境特有的安全威胁,而云计算环境特有的安全威胁又可分为恶意的hypervisor/管理员带来的安全威胁以及恶意的云用户带来的安全威胁。

1.1.1 外部安全威胁 来自外部的攻击者通常会利用云平台漏洞、网络防护不足等安全缺陷发起攻击,窃取机密信息、破坏数据的完整性以及服务的可用性。这类攻击并非云计算环境所特有的,而是在计算机系统中普遍存在,在一般的计算机系统中针对这类攻击已有成熟的解决方案,但并非所有的解决方案都适用于云计算环境。Liao等[8]于2016年利用云主机廉价以及易于部署的特点,在云计算环境中构建挂马网站、钓鱼网站以及DDoS攻击载体实现多种网络攻击,这种攻击方式一般将恶意服务部署在处于不同地理位置的云主机中,使得云计算环境难以对其进行集中安全检测与防护。Wu等[9]于2017年针对云计算环境构建了一个SQL注入的攻击场景,并就SQL注入对云计算环境数据完整性的影响进行分析。Cojocar等[10]在2020年提出利用rowhammer漏洞来实现提权,进而对用户数据进行操纵攻击。袁枫等[11]提出利用提权漏洞对微软Azure云计算环境进行渗透,进而对用户数据进行窃取、删除或篡改攻击。

1.1.2 *内部安全威胁*　随着公有云计算环境的普及,来自云计算环境内部的安全威胁不断增加,并日渐成为云计算环境所面临的主要安全威胁。

按照威胁来源,源自内部的安全威胁又可分为源自不可信管理员的安全威胁和源自恶意云用户的安全威胁。不可信管理员利用其拥有的特权窃取或破坏云租户的数据或通过提供虚假的服务(fraudulent resource consumption, FRC)使云租户"花冤枉钱"。FRC 攻击最早是由 Idziorek 等[12]提出的,其目标是剥夺云租户对其购买资源的消费能力。

来自恶意云租户的安全威胁通常有两种:共存攻击和资源窃取攻击。共存攻击通常是利用虚拟机逃逸或边信道攻击来获取邻近虚拟机的隐私信息。在 2009 年,Ristenpart 等[13]首次提出基于侧信道的虚拟机共存攻击,该攻击利用不同虚拟机之间共享数据 cache 这一特性,在亚马逊 EC2 服务器上成功构建了带宽为 0.2 b/s 的时序侧信道。在资源窃取攻击中,攻击者通过大量占用某类资源,使得相邻用户云主机中的任务因得不到足够资源而被迫停止执行,终止任务所获得的资源则被攻击者所获取。Gao 等[14]于 2019 年提出利用攻击抢占同一虚拟机中不同容器的性能,并在亚马逊 EC2 云主机上进行实验,发现攻击者容器运行效率可提升 60%。

1.2　针对 PaaS 层的安全威胁

相比于 IaaS 层,用户对 PaaS 层服务的控制能力更小。因此,相比于 IaaS 层的安全威胁,PaaS 层来自外部的安全威胁和其他用户的安全威胁较少,更多的安全威胁来自于不可信的云计算供应商本身。随着容器技术的成熟,基于容器技术的微服务模式成为 PaaS 层服务的主流模式,容器安全也逐渐成为 PaaS 层的核心安全问题。

1.2.1 *针对 PaaS 层机密性的安全威胁*　这类攻击来源有两种:不可信的 PaaS 层供应商对用户数据的窃取和其他恶意用户对受害者数据的窃取。Zhang 等[15]于 2014 年提出一种基于侧信道的跨用户信息窃取攻击,该攻击能够对 PaaS 层数据的保密性和用户隐私构成威胁,为验证攻击方案的可行性,构建了攻击示例,并利用该示例获取到 PaaS 层其他用户网站信息,包括网购平台账号信息、购物车信息等。

1.2.2 *针对 PaaS 层可用性的安全威胁*　这类攻击通常是由处于同一虚拟机中的恶意用户对其他用户的服务发起攻击。随着容器技术的兴起,微服务模式开始在 PaaS 层流行起来,而恶意用户对其他用户微服务的破坏或资源抢夺就成了 PaaS 层云服务可用性的主要威胁。Houdini 攻击就是利用同一虚拟机中各容器之间抢占 CPU、网络带宽等资源实现的一种 DoS 攻击,使得受害者容器内的微服务无法正常执行。Vissers 等[16]于 2015 年提出一种针对 PaaS 平台的 DDoS 攻击,该攻击能绕过基于云的 ip 混淆防护,从而对受害者的真实主机实现 DDoS 攻击。

1.3　针对 SaaS 层的安全威胁

SaaS 层服务需要面对的安全威胁包括对用户隐私的窃取以及对服务可用性的攻击。在 SaaS 层,用户不仅需要面对因外部的安全威胁而泄露隐私的风险,还需要面对不可信的云服务本身窃取用户数据隐私的风险。

1.3.1 *针对 SaaS 层机密性的安全威胁*　Rehman 等[17]认为,SaaS 层面对的主要安全威胁之一是用户隐私的泄露。目前,SaaS 层服务通常以终端应用的方式实现,不合理的访问控制机制使得应用获得远超服务所需的权限,进而窃取用户隐私。Zuo 等[18]发现,将云主机作为服务器后台的应用会由于对用户认证信息不合理的管理以及对用户权限的错误配置而导致用户隐私泄露。

1.3.2 *针对 SaaS 层可用性的安全威胁*　Aime 等[19]认为,对 SaaS 层可用性的安全威胁主要来自于不可信的服务提供商。不可信的服务提供商可能会篡改用户数据或为用户提供虚假服务,例如恶意的搜索引擎会给用户返回错误的、含有恶意文件的搜索结果。Guillén 等[20]对 SaaS 层安全威胁进行了更系统的研究,认为 SaaS 层主要的安全威胁包括恶意应用通过网络攻击受害者终端、恶意应用直接攻击受害者的底层终端以及恶意代理窃取用户信息等,这些攻击均来源于不可信的服务提供商。

2　可信云计算的概念

面对虚假服务、资源窃取、共存攻击等云计算环境特有的安全威胁,基于加密和软件检测的安全防护技术难以提供有效的解决方案。因此,学术界提出将可信计算技术与云计算相结合,通过构建信任链的方式从根本上解决云服务所面临的安全问题。

2.1　可信计算

可信计算的概念[21]于 1985 年提出,旨在确保计算机系统和网络空间整体的安全可信。可信计算的基本思想[22]是:在计算系统底层中创建一个可信基,基于可信基构建信任链,通过信任链传递确保系统整体的可信性。

目前,可信计算的主流实现方式是在硬件底层构建一个可信基,由硬件可信基对操作系统内核进

行度量,以此来实现信任链的传递。在国外,由可信计算组织(trusted computing group,TCG)提出的可信平台模块构建标准[23]正是这种思想的典型代表;在国内,基于此思想制定了以可信加密模块为核心的《可信计算密码支撑平台功能与接口规范》[24]系列标准。

近年来,国内外可信计算研究工作层出不穷,可信计算技术得到了长足的发展。基于TPM,IBM提出了一种适用于PC和服务器的IMA度量框架[25],该框架能在程序加载时对其进行度量,但其缺陷是系统效率较低,且无法度量程序运行时的完整性。为此,Davi等[26]于2009年提出一种基于TPM的程序动态完整性验证机制DyIMA,该方案能够实现高效、动态的程序完整性验证,将信任链有效地扩展到了软件层。

2.2 可信云计算

由于云环境的外包特性,云环境中数据以及计算实体的所有者、管理者、使用者往往并非一体。对于云用户来说,云计算环境是一个黑盒,云用户仅能获得其申请服务的最终结果,用户完全无法得知云计算环境对数据的处理是否安全可靠,云计算环境传递给用户的计算结果是否真实,云计算环境由此产生了一系列新的安全问题,如虚假服务、隐私窃取等。因此,确保云环境安全的关键就是实现可信云计算环境。

可信云计算的概念最初是由Santos等[7]提出的,其将可信计算中远程证明和信任链传递的思想引入云计算,旨在云计算中构建完整的可信环境。杨健等[27]提出基于现有可信计算技术,在云环境中建立可信计算基,以保护云计算环境的机密性、完整性。

总之,可信云计算实现的总体思路就是将现有的可信计算技术应用到云计算环境中,但这种应用不是简单的复制和移植,相比于传统的可信计算技术,可信云计算在实现时还需要考虑如下一些额外的安全问题。

1) 如何判断基础设施提供商是否可信?

2) 如何在其他云租户不可信的情况下确保正常用户服务是安全可信的?

3) 如何在管理员不可信的情况下确保云计算的过程是可信的?

上述这些问题也是实现可信云计算的关键问题。

3 可信云计算技术的发展

目前在学术界,实现可信云计算环境的主流思想主要有三种,即基于虚拟化可信基的可信云计算技术,基于可信执行环境的可信云计算技术,基于第三方认证的可信云计算技术。

可信计算技术提出的初衷就是在整个计算机系统中构建一个自下而上的信任链。然而,具体到云计算环境,可信计算从定义到实现相比于传统的服务器环境又有些许不同。其一,云计算环境中"一切皆服务",用户所使用的资源和所执行的操作皆以服务的方式实现。因此,可信云计算技术不仅要保证云计算环境中的数据可信和行为可信,还要保证服务可信。其二,因云计算的外包特性,云计算用户对底层软硬件不具备控制权限,当云计算服务商或其他的云计算用户不可信时,云计算用户所使用资源与所购买服务的安全性往往难以得到保障。因此,可信云计算技术在实现时就应当考虑在系统管理员不可信的前提下如何确保用户所购买资源或服务的可信性。

3.1 基于虚拟化可信基的可信云计算技术

虚拟化可信基的典型应用是vTPM。vTPM的概念最早是由Perez等[28]于2006年提出,其主要结构如图1所示。

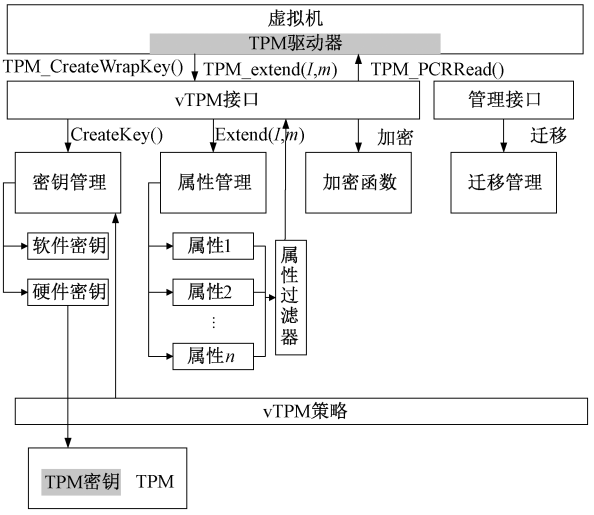

图1 vTPM的主要结构

Figure 1 The main structure of vTPM

王丽娜等[29]提出一种基于信任扩展的可信虚拟执行环境构建方法,然而该工作存在的关键问题是难以确保系统管理员的可信性。Li等[30]提出多租户可信计算环境模型(multi-tenancy trusted computing environment model,MTCEM),该模型明确了IaaS层用户和云服务提供商的安全职责。MTCEM利用可传递的可信机制构建可信计算平台,使用远程证明机制确保用户虚拟机的机密性。尽管该方案利用TPM和可信第三方保证了云平台本身的可信性,但该方案未能有效地利用TPM对用户虚拟机进

行保护,攻击者依然能够对虚拟机的状态进行破坏,进而破坏虚拟机中服务的完整性和有效性。为此,Varadharajan 等[31]提出基于属性的认证模型,利用 TPM 在用户虚拟机上建立信任链,确保用户虚拟机不会被篡改,保证了虚拟机执行事务的完整性和有效性。

通过对上述研究工作的分析,发现已有的方案还存在一些值得改进的地方,主要表现在以下两个方面。

1) vTPM 与物理 TPM 之间的映射缺乏安全保护。现有的安全机制缺乏对 vTPM 和物理 TPM 之间映射的防护,攻击者可能通过篡改虚拟 PCR 寄存器破坏虚拟机的可信基。因此,如何确保物理 TPM 和 vTPM 之间映射的安全性将是未来一段时间的研究热点。

2) vTPM 难以在虚拟机迁移时对虚拟机进行安全防护。在虚拟机迁移过程中,vTPM 需要结束与原物理机的映射,并与迁移后的物理机的 TPM 构建新的映射。因此,在迁移过程中,攻击者可能窃取虚拟机中的数据,或者使虚拟机与不安全的物理机进行映射。如何利用 vTPM 实现虚拟机的可信迁移将是未来一段时间的研究重点和难点。

3.2　基于可信执行环境的可信云计算技术

可信执行环境是 CPU 内的一个安全区域,它运行在一个独立的环境中且与操作系统并行运行。基于可信执行环境构建可信云计算的目的是确保在云计算平台管理员/hypervisor 不可信的情况下,云计算环境依旧可以为用户提供可信的服务。Schuster 等[32]提出了基于可信执行环境的云平台模型“VC3”,该模型利用 Intel SGX 技术,在云平台实现一种保密的 MapReduce 计算模型,使得用户能够在云平台执行加密的计算任务,同时能够保证计算结果的完整性。该工作有效地保护了应用层计算任务的保密性和完整性,美中不足的是该工作在 enclave 中不允许执行系统调用。因此,该方案难以保证系统调用的安全性。为了弥补 VC3 方案难以对系统调用进行保护的缺陷,Arnautov 等[33]提出了基于 SGX 的可信容器模型“SCONE”,该模型通过在 SGX 中构建可与系统进行交互的容器,实现 SGX 对系统调用的保护。

利用可信执行环境构建可信云环境存在以下一些共性的问题。

1) 目前商用化的可信执行环境所能够使用的软硬件资源较为有限,现有的可信执行环境仅能对一些关键的数据、基础的应用进行防护,或者对复杂应用的关键部分进行防护。如何扩大商用可信执行环境在云计算中的安全防护边界将是未来一段时间的研究重点。

2) 由于可信执行环境本身难以对非传统的攻击方式(如比特翻转、侧信道攻击)进行防护,因此基于可信执行环境构建的可信云服务也难以抵抗这种攻击。

3.3　基于第三方认证的可信云计算技术

使用可信第三方建立可信云计算的主要思想是建立一个第三方的权威认证中心,提供对用户的身份认证、数据传输、计算服务等的监控。Zissis 等[34]提出利用可信第三方实现云用户的数据加密、用户远程认证等功能,保护用户数据的机密性和完整性。Santos 等[7]提出利用可信云计算平台来确保云服务的有效性以及云用户数据的机密性和完整性,该方案利用可信协调中心管理云中所有节点,其创新点在于将认证端和管理端拆分开来,云计算平台针对虚拟机的任意行为都需要向可信第三方的协调中心进行认证。然而,由于云计算平台对虚拟机执行的任何操作都需要可信第三方的认证,这就必然导致云计算平台性能的显著下降。为了解决上述问题,Wang 等[35]提出一种直接匿名认证和隐私证书分发方式,减少了可信第三方的认证频率,进而降低了云计算平台的性能损耗。

现有的方案主要存在以下一些不足之处。

1) 由于利用可信第三方实现的可信云计算平台在执行操作之前需要向可信第三方进行认证,因此在可信云平台执行用户任务和管理虚拟机的过程中,不可避免地会产生通信开销和性能损耗。如何在利用可信第三方实现远端认证的同时,尽可能地降低远端认证所带来的性能损耗将是未来的研究重点。

2) 当恶意的云计算用户利用侧信道攻击(如 co-residence 攻击)窃取信息时,基于可信第三方的可信云平台既无法进行检测也无法进行防护。如何利用可信第三方实现对云平台侧信道的检测与防护将成为未来研究的难点之一。

3.4　可信云计算尚未解决的问题

目前,可信云计算技术已基本走向成熟,然而可信云计算在解决大量云计算环境安全问题的同时,还有一些安全问题在可信云计算环境中尚未出现成熟的解决方案,这些安全问题也是可信云计算接下来需要进行研究的关键。

3.4.1　*云主机的安全迁移*　云主机的安全迁移从云计算技术建立之初就是安全研究人员重点关注的

目标之一。由于云计算具有使用者和管理者分离的特性,云主机的迁移对云租户而言相当于一个黑盒过程,因此在迁移过程中用户数据的机密性难以得到保证。又由于迁移的虚拟机结构较为复杂,使得对迁移后云主机的完整性校验难以实现,因此迁移后云主机的完整性也难以保证。

为解决上述问题,安全研究人员提出了一系列解决方案[36]。Wall 等[37]提出了基于加密的云主机可信迁移技术来保证云主机迁移过程中的机密性,然而该方案成立的前提是基础设施供应商本身就是安全可信的,而这一点在公有云环境中恰恰是最难以保证的。为了在云服务提供商/管理者不可信的前提下实现云主机的可信迁移,Gu 等[38]提出基于 SGX 的云主机可信迁移方案,然而该方案依旧存在一些不足之处:首先,SGX 中 enclave 容量有限,难以支撑大范围的数据迁移,该方案仅能对一些关键数据进行保护;其次,该方案难以确保云主机迁移后状态的完整性[39]。因此,云主机的可信迁移仍然是今后一段时间的研究重点。

3.4.2 *对恶意云用户的有效检测* 对合法的云服务提供商,尤其是云基础设施提供商而言,在不破坏用户隐私的情况下检测云用户是否合法也是一件极为困难的事情。为确保用户隐私,合法的云服务提供商不会主动监控用户主机中的行为或者窥探用户的隐私数据,这就使得大量恶意用户利用云计算环境实现大规模的网络攻击,如 DDoS 攻击[40]、僵尸网络[41-42]、共存攻击[43]等。

为解决上述问题,安全研究人员提出了诸多基于非安全行为分析的恶意用户检测方案,如基于异常资源占用的共存攻击检测[44],基于异常流量分析的 DDoS 检测[45]等。然而,这些方案仅能对恶意用户的部分行为进行检测,无法全面检测恶意用户的非法行为,更难以做到有效的预防。

近年来,随着零信任概念的提出,针对零信任环境的访问控制模型应运而生,如基于上下文的访问控制[46],结合代理重加密的基于属性的细粒度访问控制[47]等。上述方案旨在零信任网络中实现通信双方的动态访问控制,以保证在不破坏用户隐私的前提下对用户的行为进行限制。这些访问控制机制为恶意云用户的检测与预防提供了一定的解决思路,但该问题仍会是今后一段时间的研究难点。

4 应用可信云计算提升云计算安全

现有的安全解决方案在面对云计算的安全威胁尤其是来自内部的安全威胁时,往往难以确保用户所使用资源与服务的可信性,而可信云计算技术通过在整个云计算环境中构建信任链,能够有效地抵御上述安全威胁,尤其是来自内部的安全威胁对云计算环境保密性、完整性、可用性的破坏。本文将从云计算各层次入手,分析可信云计算技术在确保云计算环境安全性中的作用。

4.1 可信云技术在保护 IaaS 层安全性中的作用

IaaS 层面临的主要安全威胁包括外部攻击者对云用户数据机密性、完整性和云服务可用性的破坏,以及不可信的云服务提供商对用户隐私的窃取。接下来将讨论可信云技术在解决上述安全问题时的作用。

虚拟机是 IaaS 层的重要组成部分,确保虚拟机在整个生命周期内的可信性是实现云平台可信的基础。Szefer 等[48]提出将虚拟机所需资源从 hypervisor 控制中剥离出来,并为每个虚拟机单独构建可信基的方法,消除针对 hypervisor 的攻击平面以及恶意 hypervisor 对云服务的安全威胁,使得即使 IaaS 层 hypervisor 不可信,用户虚拟机中的数据也不会受到攻击者的窃取或恶意篡改。

当虚拟机发生迁移后,确保虚拟机数据和状态的完整性是可信云计算技术需要解决的关键问题。Soriente 等[49]利用 SGX 技术以及拜占庭同步机制,在云环境中实现了一种可部署、可撤销、可转移的可信执行环境机制,使得用户能够在不同的物理机中部署相同的 enclave,以实现虚拟机的安全转移。Gu 等[38]提出一种基于 SGX 的可信云平台虚拟机迁移方案,使得存在 enclave 的虚拟机能够在 hypervisor 不可信的云环境中实现虚拟机的可信迁移,同时不会破坏 enclave 的安全防护机制。

4.2 可信云技术在保护 PaaS 层安全性中的作用

随着容器技术的逐渐成熟以及微服务的日渐兴起,产业界出现将部署在 IaaS 层的服务转变为部署在 PaaS 层微服务的趋势。与此同时,针对 PaaS 层的安全威胁,尤其是针对容器技术和微服务的安全威胁日渐增多,容器安全成为 PaaS 层安全的研究重点。此外,将容器的属性与现有的可信云技术相结合产生的云原生安全技术也成为云安全新兴的研究热点。

可信云计算通过将系统的可信链扩展到容器内部,来保证容器内数据的机密性、完整性和微服务的完整性、可用性。为保护微服务中数据的机密性、完整性,Preuveneers 等[50]提出基于多租户的微服务访问控制机制,使得用户、服务提供商均能够合法地访问微服务。该方案包括对多个利益相关者进行授权

的机制、独立可部署的认证策略以及对应的运行框架、面向策略的访问控制服务,该策略支持跨计算域的交互性。Easley 等[51]通过在操作系统中为容器构建 monitor 的方式来保证运行时容器的安全性和可信性。

在工业界,谷歌提出了基于安全隔离的轻量级容器沙箱 gVisor[52],gVisor 本质上是一个用于容器的应用内核,它限制了应用对主内核的访问权限。不同于传统的内核,gVisor 不需要固定的物理资源,利用主内核的功能并作为一个普通进程运行。

开源项目 Kata Container[53]是在普通的容器之上构建一个针对容器的 hypervisor,该 hypervisor 通过硬件虚拟化实现,每一个 Kata Container Pod 实际上是一个半虚拟机,拥有完整的 Linux 内核。Kata Container 具有强隔离性,也拥有与容器相媲美的敏捷性。

4.3　可信云技术在保护 SaaS 层安全性中的作用

相比于 IaaS 层和 PaaS 层服务,SaaS 层用户对服务的控制范围变得更小,可能遭受外部安全威胁的攻击平面也相对减小。因此,SaaS 层的安全问题更加集中于云服务/应用本身的安全性和可信性,这一点在安卓平台尤为明显。由于智能机和嵌入式设备本身计算能力的局限性,安卓平台服务的通用模型是应用仅作为用户和服务交互的接口,将大量计算和存储任务委托给云端完成,云端再将计算结果传递到应用的客户端。在这种情况下,如果作为应用"后台"的云服务遭受外部攻击或本身就是恶意的,那么用户数据的机密性和完整性以及用户所购买服务的有效性就会遭到破坏。因此,确认云服务本身的可信性是 SaaS 层安全问题的核心和重中之重。为解决应用背后云平台的可信问题,Almorsy 等[54]提出 TOSSMA 模型,该模型利用可信第三方提供的加密、认证服务,为用户提供可自定义的 SaaS 层服务的安全要求。Dijk 等[55]提出一种检查云服务中存储数据是否加密的协议,以此来检查云服务的可信性。

云计算面临的安全威胁与对应的防护方案列于表 2。

表 2　云计算面临的安全威胁与对应的防护方案

Table 2　Security threats to cloud computing and corresponding solutions

云计算层级	威胁类型	攻击	防护方案
IaaS	来自外部的安全威胁	拒绝服务攻击、ip 地址释放后重用攻击、提权攻击、恶意资源部署攻击	Soriente[49]、Gu[38]
IaaS	来自内部的安全威胁	欺骗攻击、特权攻击、共享资源攻击	Szefer[48]、Soriente[49]、Gu[38]
PaaS	针对机密性的安全威胁	侧信道攻击、特权攻击	Preuveneers[50]、Easley[51]、gVisor[52]、Kata Container[53]
PaaS	针对可用性的安全威胁	信息窃取攻击、Houdini 攻击、真实地址攻击	Preuveneers[50]、Easley[51]、gVisor[52]、Kata Container[53]
SaaS	来自外部的安全威胁	内存泄漏攻击、应用提权攻击、投毒攻击(针对机器学习)	Almorsy[54]、Dijk[55]
SaaS	来自内部的安全威胁	侧信道攻击、资源窃取攻击	Almorsy[54]、Dijk[55]

5　可信云计算的发展趋势

5.1　可信云计算实现云原生安全

云原生安全是指依托于云计算独有的技术,确保云计算的安全可信。目前一种主流观点认为,随着公有云的推广和普及,互联网企业的应用与服务将完全基于云计算技术来构建,云计算将与系统安全密不可分。一方面,为确保云计算环境基础设施的安全性,传统的安全手段必不可少;另一方面,云计算的各种新技术(如服务外包、边缘计算、联邦学习等),也在深刻变革着当前的安全技术发展路线[56]。

当前可信云计算的主要实现方式还是将传统的安全技术赋予到云计算环境中,而将云计算环境自带的特性(如虚拟化、微服务、容器)融入到传统的系统安全中尚处于探索阶段,但已初见成效。如绿盟科技提出基于云的安全服务平台,将安全防护、漏洞检测、访问控制、DDoS 防御等集成于云平台,利用可信虚拟化、微服务技术为用户提供基于云计算的安全服务。

5.2　边缘与隐私计算中的安全问题

随着嵌入式技术和物联网技术的发展,智能家居、个域网的概念逐渐普及。在万物互联的时代,不仅是服务器和个人计算机,智能机、手环、智能家居等嵌入式设备也将成为云计算环境的一部分。为了

解决云计算中心有限的计算能力和云环境中海量数据之间的矛盾,学术界提出了边缘计算的概念[57]。然而,边缘计算需要收集用户的位置、偏好等隐私信息,大大提高了用户隐私泄露的风险。为了解决该问题,学术界又提出了隐私计算的概念,常用的隐私计算技术包括全同态加密[58]、可搜索加密[59]等。然而,现有的隐私计算技术普遍存在效率较低、性能损耗过大等问题。如何提高隐私计算的性能将是未来研究的关键点。

5.3 提高可信云计算环境对非传统攻击的防护能力

针对可信云计算的现有工作普遍存在的一个不足之处是缺乏对非传统攻击(如rowHammer[60]、微指令架构缺陷攻击[61]、侧信道攻击[62])的防护能力。针对这类新型的攻击方式,学术界和工业界也提出了一些对应的解决方案,如对可能产生比特翻转的内存位置进行定期校验,对攻击者可能利用的侧信道和隐蔽信道进行加噪处理[63]等。对利用微指令架构缺陷的攻击方案(如meltdown[64]、spectre[65]),研究人员提出利用硬件检测的方式实现攻击检测与防护。然而,这些防护方案依然是针对传统的计算环境构建的。如何将这些面向传统计算环境的防护方案整合到可信云计算环境中将成为未来的研究热点。

5.4 可信云计算与机器学习的结合

云计算为机器学习提供了大量且廉价的计算与存储资源,大数据则为机器学习提供了海量的用来训练和测试的数据,云计算技术的发展进一步推动了机器学习技术的发展。然而,云计算环境本身的不安全性也为机器学习带来了额外的安全风险。例如,不安全的云计算平台可能会窃取用户的训练模型,使得机器学习的保密性受到影响;不安全的云存储服务可能会篡改用于训练模型的数据,进而破坏机器学习模型的完整性,实现投毒攻击。如何将可信云计算与机器学习结合起来,在不破坏机器学习用户隐私性、保密性的前提下实现对机器学习模型的保护将是未来研究的热点。

6 小结

本文重点介绍了当前云平台面对的主要安全问题、可信云计算的实现方式以及可信云计算在云服务安全中的作用,并探讨了可信云可能的发展趋势。总体来说,可信云计算技术为诸多云计算安全挑战提出了新的解决思路,解决了很多传统安全方案难以解决的安全问题。但随着云计算的发展,可信云计算也需要不断发展,以解决新的安全问题。

参考文献:

[1] McAfee. 2017云安全报告[EB/OL]. [2021-06-14]. https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk.html.
McAfee. 2017 cloud security report[EB/OL]. [2021-06-14]. https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk.html.

[2] 腾讯安全. 2020年公有云安全报告[EB/OL]. [2021-02-07]. https://tencent.com/research/report/1248.html.
Tencent Security. 2020 public cloud security report[EB/OL]. [2021-02-07]. https://tencent.com/research/report/1248.html.

[3] GREEN M, ATENIESE G. Identity-based proxy re-encryption[M]//Applied Cryptography and Network Security. Berlin: Springer Press, 2007: 288-306.

[4] AMBROSIN M, CONTI M, DARGAHI T. On the feasibility of attribute-based encryption on smartphone devices[C]//Proceedings of the Workshop on IoT Challenges in Mobile and Industrial Systems. New York: ACM Press, 2015: 49-54.

[5] KARNWAL T, SIVAKUMAR T, AGHILA G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack[C]//Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science. Piscataway: IEEE Press, 2012: 1-5.

[6] KOURAI K, AZUMI T, CHIBA S. A self-protection mechanism against stepping-stone attacks for IaaS clouds[C]//Proceedings of the 9th International Conference on Ubiquitous Intelligence and Computing and the 9th International Conference on Autonomic and Trusted Computing. Piscataway: IEEE Press, 2012: 539-546.

[7] SANTOS N, GUMMADI K P, RODRIGUES R. Towards trusted cloud computing[C]//Proceedings of the Workshop on Hot Topics in Cloud Computing. Berkeley: USENIX Association, 2009: 1-5.

[8] LIAO X J, ALRWAIS S, YUAN K, et al. Lurking malice in the cloud: understanding and detecting cloud repository as a malicious service[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 1541-1552.

[9] WU T Y, CHEN C M, SUN X Y, et al. A countermeasure to SQL injection attack for cloud environment[J]. Wireless personal communications, 2017, 96(4): 5279-5293.

[10] COJOCAR L, KIM J, PATEL M, et al. Are we suscepti-

ble to rowhammer? An end-to-end methodology for cloud providers[C]//Proceedings of the IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020: 712-728.

[11] 袁枫, 王轶骏, 薛质. 面向 Azure 的云平台渗透技术研究[J]. 通信技术, 2020, 53(12): 2885-2891.
YUAN F, WANG Y J, XUE Z. Cloud platform penetration technology for Azure[J]. Communications technology, 2020, 53(12): 2885-2891.

[12] IDZIOREK J, TANNIAN M, JACOBSON D. Detecting fraudulent use of cloud resources[C]//Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. New York: ACM Press,2011: 61-72.

[13] RISTENPART T, TROMER E, SHACHAM H, et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM Press, 2009: 199-212.

[14] GAO X, GU Z S, LI Z F, et al. Houdini's escape: breaking the resource rein of linux control groups[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 1073-1086.

[15] ZHANG Y, JUELS A, REITER M K, et al. Cross-tenant side-channel attacks in PaaS clouds[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2014: 990-1003.

[16] VISSERS T, VAN GOETHEM T, JOOSEN W, et al. Maneuvering around clouds: bypassing cloud-based security providers[C]//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press,2015: 1530-1541.

[17] REHMAN S, GAUTAM R. Research on access control techniques in SaaS of cloud computing[M]//Communications in Computer and Information Science. Berlin: Springer Press, 2014: 92-100.

[18] ZUO C S, LIN Z Q, ZHANG Y Q. Why does your data leak? Uncovering the data leakage in cloud from mobile apps[C]//Proceedings of the IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 1296-1310.

[19] AIME M D, LIOY A, POMI P C, et al. Security plans for SaaS[M]//New Frontiers in Information and Software as Services. Cham: Springer International Publishing, 2011: 81-111.

[20] GUILLÉN D L, MORALES-ROCHA V, MARTÍNEZ. A systematic review of security threats and countermeasures in SaaS[J]. Journal of computer security, 2020, 28(6): 635-653.

[21] BELL J P. Department of defense trusted computer system evaluation criteria[M]. London: Palgrave Macmillan Press, 1985.

[22] 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, 40(2): 139-166.
SHEN C X, ZHANG H G, WANG H M, et al. Research and development of trusted computing[J]. Scientia sinica (informations), 2010, 40(2): 139-166.

[23] Trusted Computing Group. TCG specification architecture overview[EB/OL]. [2021-03-02]. https://trustedcomputinggroup.org/wp-content/uploads/TCG_1_4_Architecture_Overview.pdf.

[24] 中国国家标准化管理委员会. 信息安全技术 可信计算密码支撑平台功能与接口规范: GB/T 29829—2013[S]. 北京: 中国标准出版社, 2014.
Standardization Administration of China. Information security techniques: functionality and interface specification of cryptographic support platform for trusted computing: GB/T 29829—2013[S]. Beijing: Standards Press of China, 2014.

[25] SAILER R, ZHANG X, JAEGER T, et al. Design and implementation of a TCG-based integrity measurement architecture[C]//Proceedings of the 13th Conference on USENIX Security Symposium. Berkeley: USENIX Association, 2004: 223-238.

[26] DAVI L, SADEGHI A R, WINANDY M. Dynamic integrity measurement and attestation: towards defense against return-oriented programming attacks[C]//Proceedings of the ACM Workshop on Scalable Trusted Computing. New York: ACM Press,2009: 49-54.

[27] 杨健, 汪海航, 王剑, 等. 云计算安全问题研究综述[J]. 小型微型计算机系统, 2012, 33(3): 472-479.
YANG J, WANG H H, WANG J, et al. Survey on some security issues of cloud computing[J]. Journal of Chinese computer systems, 2012, 33(3): 472-479.

[28] PEREZ R, SAILER R, VAN D L. vTPM: virtualizing the trusted platform module[C]//Proceedings of the 15th Conference on USENIX Security Symposium. Berkeley: USENIX Association,2006: 305-320.

[29] 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.

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

[31] VARADHARAJAN V, TUPAKULA U. Counteracting security attacks in virtual machines in the cloud using property based attestation[J]. Journal of network and computer applications, 2014, 40(1): 31-45.

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

[33] ARNAUTOV S, TRACH B, GREGOR F, et al. SCONE: secure linux containers with intel SGX[C]//Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation. Berkeley: USENIX Association,2016: 689-703.

[34] ZISSIS D, LEKKAS D. Addressing cloud computing security issues[J]. Future generation computer systems, 2012, 28(3): 583-592.

[35] WANG H Z, HUANG L S. An improved trusted cloud computing platform model based on DAA and privacy CA scheme[C]//Proceedings of the International Conference on Computer Application and System Modeling. Piscataway: IEEE Press, 2010: 13-33.

[36] SIGHOM J N, ZHANG P, YOU L. Security enhancement for data migration in the cloud[J]. Future internet, 2017, 9(3): 23-35.

[37] WALL M. Can we trust cloud providers to keep our data safe? [EB/OL].[2021-03-21]. http://www.bbc.com/news/business-36151754.

[38] GU J Y, HUA Z C, XIA Y B, et al. Secure live migration of SGX enclaves on untrusted cloud[C]//Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE Press,2017: 225-236.

[39] ALDER F, KURNIKOV A, PAVERD A, et al. Migrating SGX enclaves with persistent state[C]//Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE Press, 2018: 195-206.

[40] SOMANI G, GAUR M S, SANGHI D, et al. DDoS attacks in cloud computing: issues, taxonomy, and future directions[J]. Computer communications, 2017, 107: 30-48.

[41] CLARK K, WARNIER M, BRAZER F M T. The future of cloud-based botnets? [C]//Proceedings of the 1st International Conference on Cloud Computing and Services Science. Setúbal: Science and and Technology Publications, 2011: 597-603.

[42] KEBANDE V R, VENTER H S. A cloud forensic readiness model using a botnet as a service[C]//Proceedings of the International Conference on Digital Security and Forensics. Berlin: Springer Press, 2014: 23-32.

[43] ATYA A O F, QIAN Z, KRISHNAMURTHY S V, et al. Malicious co-residency on the cloud: attacks and defense[C]//Proceedings of the IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2017: 1-9.

[44] BATES A, MOOD B, PLETCHER J, et al. Detecting co-residency with active traffic analysis techniques[C]//Proceedings of the ACM Workshop on Cloud Computing Security Workshop. New York: ACM Press, 2012: 1-12.

[45] OSANAIYE O, CHOO K K R, DLODLO M. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework[J]. Journal of network and computer applications, 2016, 67: 147-165.

[46] LUKASEDER T, HALTER M, KARGL F. Context-based access control and trust scores in zero trust campus networks[J]. Sicherheit, 2020,10(4):53-66.

[47] YU S C, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//Proceedings of the International Conference on Computer Communications. Piscataway: IEEE Press,2010: 1-9.

[48] SZEFER J, KELLER E, LEE R B, et al. Eliminating the hypervisor attack surface for a more secure cloud[C]//Proceedings of the 18th ACM Conference on Computer and Communications Security. New York: ACM Press,2011: 401-412.

[49] SORIENTE C, KARAME G, LI W T, et al. ReplicaTEE: enabling seamless replication of SGX enclaves in the cloud[C]//Proceedings of the IEEE European Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 158-171.

[50] PREUVENEERS D, JOOSEN W. Towards multi-party policy-based access control in federations of cloud and edge microservices[C]//Proceedings of the IEEE European Symposium on Security and Privacy Workshops. Piscataway: IEEE Press, 2019: 29-38.

[51] EASLEY L G, MARTIN R L. System and method for providing container security: US7098784[P]. 2006-08-29.

[52] YOUNG E G, ZHU P, CARAZA H T, et al. The true cost of containing: a gVisor case study[C]//Proceedings of the 11th USENIX Workshop on Hot Topics in Cloud Computing. Berkeley: USENIX Association,2019:1-10.

[53] RANDAZZO A, TINNIRELLO I. Kata Containers: an emerging architecture for enabling MEC services in fast and secure way[C]//Proceedings of the 6th International Conference on Internet of Things: Systems, Management and Security. Piscataway: IEEE Press, 2019: 209-214.

[54] ALMORSY M, GRUNDY J, IBRAHIM A S. TOSSMA: a tenant-oriented SaaS security management architecture [C]//Proceedings of the IEEE 5th International Conference on Cloud Computing. Piscataway: IEEE Press, 2012: 981-988.

[55] DIJK M, JUELS A, OPREA A, et al. Hourglass schemes: how to prove that cloud files are encrypted[C]// Proceedings of the ACM Conference on Computer and Communications Security. New York: ACM Press,2012: 265-280.

[56] 刘文懋.云安全的下半场:原生安全[J]. 中国计算机学会通讯,2020,16(12): 1-10.
LIU W M. The second half of cloud security: native security [J]. Communications of the CCF, 2020, 16(12): 1-10.

[57] SHI W S, CAO J, ZHANG Q, et al. Edge computing: vision and challenges[J]. IEEE internet of things journal, 2016, 3(5): 637-646.

[58] GENTRY C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[59] WANG C, CAO N, REN K, et al. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE transactions on parallel and distributed systems, 2012, 23(8): 1467-1479.

[60] KIM Y, DALY R, KIM J, et al. Flipping bits in memory without accessing them: an experimental study of DRAM disturbance errors [C]//Proceedings of the ACM/IEEE 41st International Symposium on Computer Architecture. Piscataway:IEEE Press,2014: 361-372.

[61] SEMAL B, MARKANTONAKIS K, AKRAM R N, et al. A study on microarchitectural covert channel vulnerabilities in infrastructure-as-a-service[C]//Proceedings of the International Conference on Applied Cryptography and Network Security. Cham: Springer International Publishing, 2020: 360-377.

[62] ZHAO M, SUH G E. FPGA-based remote power side-channel attacks[C]//Proceedings of the IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2018: 229-244.

[63] BROTZMAN R, LIU S, ZHANG D F, et al. CaSym: cache aware symbolic execution for side channel detection and mitigation[C]//Proceedings of the IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 505-521.

[64] LIPP M, SCHWARZ M, GRUSS D, et al. Meltdown: reading kernel memory from user space[C]//Proceedings of the 27th USENIX Security Symposium. Berkeley: USENIX Association,2018: 973-990.

[65] KOCHER P, HORN J, FOGH A, et al. Spectre attacks: exploiting speculative execution[C]//Proceedings of the IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 1-19.