DOI:10.16515/j.cnki.32-1722/n.2020.04.003

边缘计算中的安全与隐私保护技术研究

王倩倩

(金陵科技学院软件工程学院,江苏 南京 211169)

摘 要:边缘计算在靠近物或者数据源头的物联网边缘侧就近提供智能服务,具有边缘化、移动性、分布式、虚拟化、资源动态性等特征,但它提供不了可信、可控、可用的存储与计算服务,在安全与隐私保护方面面临诸多挑战。从边缘计算环境下安全与隐私保护技术的需求出发,对该环境下身份认证、访问控制以及入侵检测等主要技术领域的研究进展进行了综述,分析并比较了典型方案的特点,讨论了已有工作的局限性,指出了未来发展趋势和后续研究方向。

关键词:边缘计算;数据安全;隐私保护;物联网

中图分类号:TN929.5 **文献标识码**:A **文章编号**:1672-755X(2020)04-0011-07

Research on Data Security and Privacy-preserving Technology in Edge Computing

WANG Qian-qian

(Jinling Institute of Technology, Nanjing 211169, China)

Abstract: Edge computing, which deploys the cloud services in the edge network, has been envisioned as the dominant cloud service paradigm in the era of IoT. Meanwhile, edge computing's unique features, such as content perception, real-time computing, parallel processing, etc., have also introduced new security problems, especially data security and privacy issues. Protecting the security and privacy of data, data owners, and data applications in such an untrusted system is thus a new challenge we are facing. From the perspective of security and privacy-preserving technologies in edge computing, this paper first introduces related research progress of identity authentication, access control and intrusion detection, and so on. Furthermore, it analyzes the characteristics and application scopes of typical schemes, and finally, the paper discusses current limitations and possible directions for future researches.

Key words: edge computing; data security; privacy-preserving; IoT

近年来,以大数据、机器学习、深度学习为代表的智能技术已经在语音识别、图像识别、用户画像等方面得到了广泛应用,该智能技术在关于算法、模型、架构等方面的研究已取得了较大的进展[1]。然而,为了满足智能化在边缘侧的各种应用需求,需要建立有效的物理世界与数字世界的连接和互动机制,构建模型驱动的智能分布式架构与平台,提供开发与部署运营的服务框架,并实现数据处理和分析的安全与隐私保护[2]等。传统的基于云计算的架构难以满足上述需求,需要边缘计算与云计算在网络、业务、应用和智能

收稿日期:2020-10-23
基金项目:中国博士后科学基金面上项目(SBH190015);江苏省普通高校研究生科研创新计划项目(KYCX18_0887)
作者简介:王倩倩(1981—),女,江苏扬州人,讲师,博士,主要从事物联网、边缘计算等研究。

方面进行协同。因此，近年来关于边缘计算的研究热度持续上升，而作为边缘计算中的核心问题，即数据安全与隐私保护问题的研究一直是其中的热点和难点。尤其随着5G通信与物联网技术在各个产业领域中的深度介入，边缘用户对数据安全与隐私保护的需求显得更为迫切，所以该领域的研究具有一定的战略性、基础性和前瞻性，其对边缘计算与未来网络技术的发展具有十分重要的意义。

本文将从信息安全的三个基本属性出发，分析边缘计算的特征和面临的安全问题，讨论边缘计算安全的系统架构，综述安全与隐私保护的关键技术，探索并构建边缘环境下一个可控、可信、可用的数据安全与隐私保护系统，以推动物联网技术、5G通信技术以及人工智能技术等的实际应用。

1 边缘计算架构与安全特征

边缘计算是将云计算平台从网络中心迁移到网络边缘，从而达到降低终端业务的端到端交付时延，抑制网络拥塞，发掘无线网络的内在潜力，提升用户体验感并促进业务创新的目的[3]。基于边缘计算技术实现的移动业务具备本地化、近距离、低时延、位置感知及网络信息感知等特点，其可以利用部署于网络边缘的计算资源，向各种应用服务提供生产运行环境，实现原有业务的“下沉”[4]。在5G通信、物联网技术等的共同助力下，未来边缘计算具有广阔的应用前景。从概念上来讲，边缘计算靠近物或数据源头的网络边缘侧，是融合网络、计算、存储、应用核心能力的分布式开放平台，它就近提供边缘智能服务，满足行业数字化在敏捷连接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求[5]。此外，它还可以作为连接物理和数字世界的桥梁，从而实现智能资产、智能网关、智能系统和智能服务，其基本架构如图1所示。

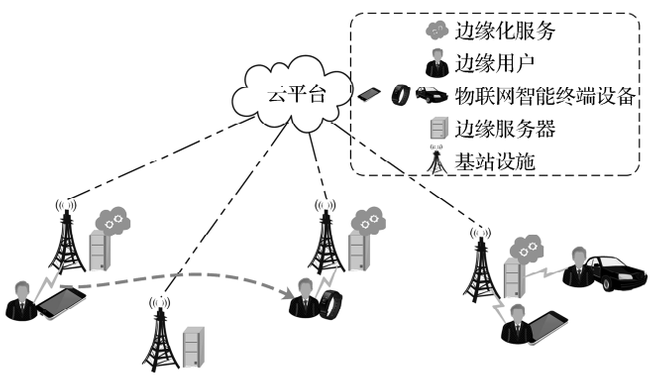

图1 物联网边缘计算基本架构示意图

显而易见，安全跨越云计算和边缘计算之间的纵深，需要实施端到端防护。在边缘数据安全中，最为关键的是如何保障数据的安全性、隐私性。然而，由于网络边缘侧更贴近万物互联的设备，其网络结构具有边缘化、移动性、分布式、虚拟化、资源动态性等特征，使得它提供不了安全可信的存储与计算服务[6]。

2 边缘计算安全与隐私保护研究现状

目前，针对边缘环境中安全与隐私保护的研究成果众多，由于不同边缘计算模式如雾计算(fog computing，FC)、移动边缘计算(mobile edge computing，MEC)、移动云计算(mobile cloud computing，MCC)等具有相似性，他们对安全与隐私保护的需求具有一定的共性[7]，因此本文将对不同边缘计算架构的研究进行梳理和分析，扩宽思路，起借鉴作用，具体如表1所示。

表1 边缘计算安全与隐私保护问题的研究分类情况

项目	云计算	雾计算(FC)	移动边缘计算(MEC)	移动云计算(MCC)	其他类型
身份认证	—	[11]	—	[10,12-13]	[9,14-16]
访问控制	—	[18-21]	[17,26-27]	[22-25]	—
信任管理	[28]	[33-34]	[32]	[29-30,35]	[31]
入侵检测	[38]	[39-41]	—	[36-37]	—
隐私保护	[43,47,49]	[44]	[51]	[42,46,48,50]	[45]

注：表中数值为文献序号。

2.1　边缘计算下的身份认证技术

在云计算和点对点计算等相关领域中已经有很多的研究成果可以为我们提供借鉴[8]。文献[9]指出点对点计算可以提供相互认证,而不必连接到中央认证服务器,因此这些方法也同样适用于处理不同信任域中边缘数据中心的身份认证问题。Donald 等人针对 MCC 架构定义了一个集中式管理的基础设施[10],其中一个可信的第三方作为认证服务器。Ibrahim 在文献[11]中开发了一个适用于雾计算的用户认证系统,允许任何边缘用户与雾节点相互认证,但这种方法需要所有的雾节点,需要存储信任域内用户的证书信息。

有研究人员提出了使用特定位置信息进行身份认证的方案。例如,在移动云计算领域中,Xu 等人介绍了情境认证的概念[12],它基于“你与谁在一起”、“你在哪里”以及“现在是几点”等相关信息进行身份认证。Bouzefrane 等人在文献[13]中使用 NFC 来验证移动设备是否将任务卸载到已授权的本地云端中。由于基于位置认证的方法已经在其他领域中得到充分研究,所以其研究成果可为边缘环境的探究提供技术参考。

一些协议试图在计算迁移场景中实现安全和高效的移动认证。例如,Yang 等人提出了一种有效的移动认证方案[14],该方案允许移动客户端从一个地区迁移到另一个地区。文献[15]则提出了一种关于弹性身份验证和授权框架的研究,该研究旨在增强在 DoS 攻击或故障情况下 IoT 服务的可用性,该方法利用了安全迁移技术,允许 IoT 设备在其自身的本地授权服务不可用时,迁移到另一台受信任的边缘服务器。但是这类协议通常需要访问集中式云基础设施中的认证服务器,需要针对边缘计算的分布式特性进行改进,所以利用区块链技术进行身份认证也是一种可行的方案,如文献[16]在边缘计算的基础上设计了一种结合访问控制机制的基于区块链技术的身份管理方案,利用认证密码技术实现网络实体的注册认证。

2.2　边缘计算下的访问控制技术

在访问控制方面,Vassilakis 等人在文献[17]中定义了一种简单的访问控制结构,使用常规的方法来部署 MEC 的安全组件,这些组件为各种 MEC 服务(如无线资源和虚拟服务)提供保护和访问控制。Dsouza 等人提出了一种针对雾计算的访问控制策略管理模型[18],在此模型中,雾体系结构的分层由策略管理模块支持,该模块定义了各种组件,包括规则库、属性数据库和会话管理库等。此外,基于属性的加密技术在访问控制中的应用得到了广泛研究,如 Wen 等人将雾计算与电网系统相结合提出了一种多权限 CP-ABE 撤销方案[19],解决了用户节点存储设备算力不足、存储空间受限的问题。Jiang 等人在 CP-ABE 方案中引入一种新机制解决了访问控制中用户身份验证和授权问题[20]。Li 等人基于雾计算的原始性特点,提出了一种新的加密机制,并构建了具体的方案[21]。Jamal 等人提出了一种新的 ABE 使用机制[22],以应对单个证书颁发机构和不相交属性颁发机构在验证用户身份授权时出现的单点故障,同时也改善了用户作业的响应时间。

在移动云计算方面,Roy 等人将移动云模型应用于医疗系统中,提出了一种可用于多服务器数据的细粒度访问控制路径以及移动云用户间的安全相互身份验证的方案[23]。Nguyen 等人提出了一个新的医疗信息系统共享框架[24],该框架在移动云平台上结合了区块链和去中心化的文件系统,设计了一种可信赖的通道并使用智能合约来控制机制,以实现不同患者与医疗提供者之间的安全电子病历共享。Zhang 等人利用了多种加密机制来设计移动云计算中安全高效的数据分发系统[25],与传统的云数据存储系统相比,该系统提供了一种轻量级且易于部署的解决方案。在移动边缘计算的访问控制方面,研究热点主要集中在车联网领域。Qi 等人提出了一种用于移动边缘计算辅助的车载网络体系结构和准入控制机制,可以大大减少服务时迟,提高有效吞吐量并帮助车载网络发挥更大潜力[26]。Li 等人在无线接入网内部部署特定的服务器,使其与道路旁的一组基站(路测单元)连接,通过利用可用的道路信息和服务器的增强功能来进一步研发针对时间的车辆切换机制,以满足车联网对高移动性和可靠性的需求[27]。

2.3　边缘计算下的信任管理机制

一些关于其他类型网络架构的研究成果可以被借鉴到边缘环境中来,例如,Petri 等人研究了如何利用各种节点来创建一个可信任的点对点云,其中反馈聚合被用来识别隐私用户[28]。此外,Chen 等人分析

了如何使用呼叫模式来推导用户之间的信任关系[29]。Hussain 等人对如何计算边缘数据中心的信任度(可信程度)进行了研究[30],提出并实现了一种集中式的信任管理结构,该结构存储了 LTE 部署在云端的信任值,用户可以使用这个结构对云服务进行匿名评价。

针对物联网边缘环境,Yuan 等人提出了一种用于评估物联网边缘设备可靠性的混合信任管理方案[31],其中,边缘设备的信任值由与其他设备的交互以及该设备所提供的服务质量进行计算,对恶意攻击者具有很好的抵抗能力。Ruan 等人提出了一种物联网中边缘环境下的信任管理框架[32],该框架可以评估应用程序及计算资源的可信程度。Junejo 等人提出了一种基于雾计算的轻量级信任管理系统[33],其中,受到安全性威胁的节点可以通过增加或者减少其他节点的信任度来提高计算模型的准确度,进而抵抗单个节点的恶意行为。Cinque 等人提出了一种雾边缘环境下物联网中基于区块链的信任管理方案[34],该方案强调虽然信任管理在物联网中十分重要,然而高能耗的信任管理难以应用到物联网传感层中资源受限的设备上。Kammoun 等人提出了一种基于信任管理和边缘计算的集群机制[35],该机制通过排查恶意节点的方式来提高系统的安全性,并通过在高评分节点之间传递可靠信息来支持信任管理。

2.4 边缘计算下的入侵检测技术

部分研究者针对边缘计算提出了具有针对性的研究方案。如 Gai 等人提出了一种针对移动云计算的入侵检测框架[36],通过使用 5G 通信的移动设备,将其入侵检测任务委托给云中的集中式服务器。Shi 等人提出了一种部署在移动云网格体系结构中的分布式 IDS[37],在该体系结构中,云端的成员可以相互协作并可与外部实体进行协作,以检测恶意软件、恶意攻击等。对于那些不需要集中式基础设施的 IDS 方案,如 Pitropakis 等人开发的 CROW 解决方案[38],该方案利用 GPU 的计算能力来有效地监控每个虚拟机的健康状况,同时检测是否存在针对基础性设施和内部人员的恶意攻击。

在雾计算领域,文献[39]针对基于雾计算的物联网环境,提出了一种用于分布式入侵检测的 LSTM 网络方案,该方案能够有效识别并分析针对物联网设备的关键攻击和威胁,并着重识别和分析了关于无线通信漏洞方面的攻击。文献[40]同样针对雾计算的物联网应用场景,提出了一种基于 OS-ELM 的入侵检测技术,该技术能够智能化地跟踪并发现物联网流量中的攻击行为。文献[41]提出了一种新的分层分布式入侵检测系统方案(HD-IDS),该方案基于分布式雾计算架构,在每个网络级别实现一个独立的 IDS 系统。

2.5 边缘计算下的隐私保护技术

云计算领域中关于隐私保护的研究也是目前的热点和难点,研究者提出了多种关于云计算的隐私保护方案[42-43],这些机制的计算开销并不高,因此他们可以被应用于边缘数据中心交互的用户设备中。

在边缘计算环境中,隐私保护技术一直是近几年备受关注的一个研究领域,为了实现隐私保护,许多安全协议[44-45]允许用户以匿名的方式与边缘数据中心及其他实体进行交互。此外,还存在专门为移动云计算环境开发的数据隐私机制,如 Ravichandran 等人提出了在合作移动设备之间关于移植代码和移植数据的隐私策略[46],并通过建立点对点交换方式,隐藏处在相同地理区域内的客户端位置网络。Huang 等人开发了利用车辆网络软件定义的匿名系统,该系统则充分利用了互联本地云的概念来实现车辆信息的隐私保护[47]。这些隐私保护方案是为本地设备的协作云设计的,他们只需所有设备相互连接,就能知道其物理位置,因此,他们也可以为协作边缘数据中心的隐私机制设计提供一些参考,在用户与位与其附近的边缘数据中心存在信任关系的情况下,可以在边缘数据中心部署隐私保护机制来帮助用户实现数据隐私保护[48-49]。另外,隐私保护技术还需要实现其他方面的隐私服务,例如通过创建匿名或隐藏他们的地址来保护用户的身份不受其他远程服务的影响[50]。文献[51]研究了无线任务迁移过程中的位置隐私和使用模式识别隐私,提出了一种基于约束马尔可夫决策过程的工作负载调度算法,该算法在保证最佳时迟和最佳能耗性能的同时,还能保持预先指定的隐私级别。

3 存在的问题与未来研究方向

边缘计算是一种新型计算模型,这种模型部署在靠近数据源头的网络边缘侧,由于其位于云与数据源

之间，因此它既可以承载来自云计算平台的下行数据，也可以面向为互联服务的上行数据。虽然，目前国内外基于边缘环境下安全与隐私保护技术方面的研究已取得了一系列的重要成果，但这一领域仍有许多具有挑战性的问题值得进一步探讨。

首先，需要保证提供的边缘计算环境在用户数据安全与隐私保护方面是可信和可控的，能够对用户的数据进行有效的安全与隐私保护。这方面的研究可以充分借鉴传统网络和云计算环境等的研究成果，通过应用传统安全与隐私保护技术，结合边缘计算场景，提出边缘环境下的有效安全与隐私保护方案，以满足用户在数据安全与隐私方面的基本需求。

其次，边缘计算环境在提供高效可用的数据安全与隐私保护方法的同时，应充分发挥边缘计算的低时延和低能耗特性，解决用户对实时性与高效性的需求问题。边缘计算技术产生的根本原因之一是为了解决现有云计算模式中心化和高时延等问题，并在用户侧提供高效的、低时延的本地化服务。安全与隐私保护技术的设置应该以边缘计算技术为前提，充分考虑边缘节点的角色定位和性能指标，为用户提供轻量级、高效率、低时延的安全与隐私保护机制。

第三，要充分考虑边缘环境的复杂性，用户需求的多样性，研究解决边缘环境下的信息安全与隐私分级保护方面的问题。这就需要提炼不同应用场景、不同数据标准、不同用户类型对安全与隐私保护的需求差异，从数据加密、通信保障、计算迁移等多个环节入手，构建分级制的安全与隐私保护模型架构，兼顾边缘应用通信质量参数与数据安全隐私需求等级，构建能满足不同类型需求的个性化及差异化的安全与隐私保护机制。

4　结　语

边缘计算作为一种新型的计算模式，能够在网络边缘侧为用户提供存储、计算、通信等服务，但是由于边缘环境的自身特点使得该环境下的安全与隐私保护技术面临诸多挑战。本文从边缘计算环境下数据的存储安全、共享安全、计算安全、传播和管控以及隐私保护等问题入手，对该领域的研究现状进行了全面综述，对其中的典型方案进行了详细介绍，并在此基础上总结了现有研究中存在的主要问题，提出了该领域的未来研究方向。

参考文献：

[1] Zhou Z，Chen X，Li E. Edge intelligence：paving the last mile of artificial intelligence with edge computing[J]. Proceeding of the IEEE，2019，107(8)：1738－1749

[2] 边缘计算产业联盟. 边缘计算参考架构 3.0 [EB/OL]. (2019－02－25)[2020－07－15]. http://www.ecconsortium.com/Uploads/file/20190225/1551059767474697

[3] Abbas N，Zhang Y，Taherkordi A，et al. Mobile edge computing：a survey[J]. IEEE Internet of Things Journal，2018(1)：450－465

[4] 施巍松，孙辉，曹杰，等. 边缘计算：万物互联时代新型计算模型[J]. 计算机研究与发展，2017，54(5)：907－924

[5] Sitton I，Alonso R S，Corchado J，et al. A review of edge computing reference architectures and a new global edge proposal[J]. Future Generation Computer Systems，2019，79(4)：278－294

[6] Roman R，Lopez J，Mambo M. Mobile edge computing：a survey and analysis of security threats and challenges[J]. Future Generation Computer Systems，2018，78(2)：680－698

[7] Xiao Y，Jia Y，Liu C，et al. Edge computing security：state of the art and challenges[J]. Proceeding of the IEEE，2019，107(8)：1608－1631

[8] Toosi A N，Calheiros R N，Buyya R. Interconnected cloud computing environments：challenges，taxonomy and survey[J]. ACM Computing Surveys，2014，47(1)：1－7

[9] Touceda D S，Cámara J M S，Zeadally S，et al. Attribute-based authorization for structured peer-to-peer(P2P) networks [J]. Computer Standards & Interfaces，2015，42(3)：71－83

[10] Donald A C，Arockiam L. A secure authentication scheme for MobiCloud[C]. Coimbatore：Proceeding of IEEE International Conference on Computer Communication and Informatics，2015：1－6

[11] Ibrahim M H. Octopus:an edge-fog mutual authentication scheme[J]. International Journal of Network Security,2016,18(6):1089－1101

[12] Xu S,Ratazzi E P,Du W. Security architecture for federated mobile cloud computing[M]. Berlin:Springer,2016

[13] Bouzefrane S,Mostefa B. Cloudlets authentication in NFC-based mobile computing[C]. Oxford:Proceeding of IEEE International Conference on Mobile Cloud Computing,Services and Engineering,2014:267－272

[14] Yang X,Huang X,Liu J K. Efficient handover authentication with user anonymity and untraceability for mobile cloud computing[J]. Future Generation Computer Systems,2016,76(4):190－195

[15] Hokeun K,Eunsuk K,David B. Resilient authentication and authorization for the internet of things(IoT) using edge computing[J]. ACM Transactions on Internet Things,2020(3):1－27

[16] Ren Y,Zhu F,Qi J,et al. Identity management and access control based on blockchain under edge computing for the industrial internet of things[J]. Applied Sciences,2019(9):1－16

[17] Vassilakis V,Chochliouros I P. Security analysis of mobile edge computing in virtualized small cell networks[C]. Rhodes:Proceeding of Conference on Artificial Intelligence Applications and Innovations,2016:653－665

[18] Dsouza C,Ahn G J,Taguinod M. Policy-driven security management for fog computing:preliminary framework and a case study[C]. San Francisco:Proceeding of IEEE International Conference on Information Reuse and Integration,2015:16－23

[19] Wen M,Chen S,Lu R,et al. Security and efficiency enhanced revocable access control for fog-based smart grid system [J]. IEEE Access,2019(7):137968－137981

[20] Jiang Y,Susilo W,Mu Y,et al. Cipher text-policy attribute-based encryption against key-delegation abuse in fog computing[J]. Future Generation Computer Systems,2018,78(2):720－729

[21] Li D,Liu J,Wu Q,et al. Efficient CCA2 secure flexible and publicly-verifiable fine-grained access control in fog computing[J]. IEEE Access,2019(7):11688－11697

[22] Jamal F,Abdullah M T,Hanapi Z M,et al. Reliable access control for mobile cloud computing(MCC) with cache-aware scheduling[J]. IEEE Access,2019(7):165155－165165

[23] Roy S,Das A K,Chatterjee S,et al. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications[J]. IEEE Transactions on Industrial Informatics,2018,15(1):457－468

[24] Nguyen D C,Pathirana P N,Ding M,et al. Blockchain for secure EHRs sharing of mobile cloud based e-health systems [J]. IEEE Access,2019(7):66792－66806

[25] Zhang J,Zhang Z,Guo H. Towards secure data distribution systems in mobile cloud computing[J]. IEEE Transactions on Mobile Computing,2017,16(11):3222－3235

[26] Qi Y,Tian L. Mobile edge computing-assisted admission control in vehicular networks:the convergence of communication and computation[J]. IEEE Vehicular Technology Magazine,2018,14(1):37－44

[27] Li L,Li Y,Hou R. A novel mobile edge computing-based architecture for future cellular vehicular networks[C]. San Francisco:Proceeding of IEEE Wireless Communications and Networking Conference,2017:1－6

[28] Petri I,Rana O F,Rezgui Y,et al. Trust modelling and analysis in peer-to-peer clouds[J]. International Journal of Cloud Computing,2012(1):221－239

[29] Chen S,Wang G,Jia W. A trust model using implicit call behavioral graph for mobile cloud computing[M]. Berlin:Springer,2013

[30] Hussain M,Almourad B M. Trust in mobile cloud computing with LTE-based deployment[C]. Bali Island:Proceeding of IEEE International Conference on Autonomic and Trusted Computing,2014:643－648

[31] Yuan J,Li X. A reliable and light weight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion[J]. IEEE Access,2018(6):23626－23638

[32] Ruan Y,Durresi A,Uslu S. Trust assessment for internet of things in multi-access edge computing[C]. Taiwan:Proceeding of IEEE International Conference on Advanced Information Networking and Applications,2018:1155－1161

[33] Junejo A K,Komninos N,Sathiyanarayanan M,et al. Trustee:a trust management system for fog-enabled cyber physical systems[J]. IEEE Transactions on Emerging Topics in Computing,2020,20(2):99－110

[34] Cinque M,Esposito C,Russo S. Trust management in fog/edge computing by means of blockchain technologies[C]. Halifax:Proceeding of IEEE International Conference on Internet of Things,2018:1433 - 1439

[35] Kammoun N,Abassi R. Towards a new clustering algorithm based on trust management and edge computing IoT[C]. Morocco: Proceeding of IEEE International Conference on Wireless Communications Mobile Computing, 2019: 1570 - 1575

[36] Gai K,Qiu M,Tao L,et al. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G[J]. Security & Communication Networks,2016,16(9):3049 - 3058

[37] Shi Y,Abhilash S,Kai H. Cloud letmesh for securing mobile clouds from intrusions and network attacks[C]. San Francisco:Proceeding of IEEE International Conference on MCC,Services and Engineering,2015:109 - 118

[38] Pitropakis N,Lambrinoudakis C,Geneiatakis D. Till all are one:towards a unified cloud IDS[M]. Berlin:Springer,2015: 136 - 149

[39] Diro A,Chilamkurti N. Leveraging LSTM networks for attack detection in fog-to-things communications[J]. IEEE Communications Magazine,2018,56(9):124 - 130

[40] Prabavathy S,Sundarakantham K,Shalinie S M. Design of cognitive fog computing for intrusion detection in internet of things[J]. Journal of Communications and Networks,2018,20(3):291 - 298

[41] Chekired D A,Khoukhi L,Mouftah H T. Fog-based distributed intrusion detection system against false metering attacks in smart grid[C]. Shanghai:Proceeding of IEEE International Conference on Communications,2019:1 - 6

[42] Zhang H,Yu N,Wen Y. Mobile cloud computing based privacy protection in location-based information survey applications[J]. Security & Communication Networks,2015(6):1006 - 1025

[43] Pietro R,Lombardi F. Security for cloud computing[M]. Boston:Artec House,2015

[44] Stojmenovic I,Wen S,Huang X,et al. An overview of fog computing and its security issues[J]. Concurrency & Computation Practice & Experience,2016,28(10):2991 - 3005

[45] Chen L,Urian R. DAA-A:direct anonymous attestation with attributes[M]. Berlin:Springer International Publishing,2015

[46] Ravichandran K,Gavrilovska A,Pande S. PiMiCo:privacy preservation via migration in collaborative mobile clouds[C]. Hawaii:Proceeding of IEEE International Conference on System Sciences,2015:5341 - 5351

[47] Huang X,Yu R,Kang J,et al. Software defined networking with pseudonym systems for secure vehicular clouds[J]. IEEE Access,2016(4):3522 - 3534

[48] Seneviratne S,Seneviratne A,Mohapatra P. Personal cloudlets for privacy and resource efficiency in mobile in APP advertising[C]. Bangalore:Proceeding of International Workshop on Mobile Cloud Computing & Networking,2013: 33 - 40

[49] Page A,Kocabas O,Ames S,et al. Cloud-based secure health monitoring:optimizing fully-homomorphic encryption for streaming algorithms[C]. Austin:Proceeding of IEEE Global Communications Workshops,2014:48 - 52

[50] Takabi H,Zargar S T,Joshi J B D. Mobile cloud computing and its security and privacy challenges[J]. Cloud Technology:Concepts,Methodologies,Tools and Applications,2015(3):1561 - 1584

[51] He X,Liu J,Jin R. Privacy-aware offloading in mobile-edge computing[C]. Singapore:Proceeding of IEEE Global Communications Conference,2017:1 - 6

(责任编辑:谭彩霞)