DOI:10.13196/j.cims.2019.12.006

边缘计算安全综述与展望

陶耀东[1,3],徐 伟[2],纪胜龙[3]
(1.北京交通大学,北京 100000;2.中国科学技术大学,安徽 合肥 230031;
3.奇安信科技集团股份有限公司,北京 100000)

摘 要:随着信息通信技术和物联网技术的发展,连接网络的设备数和产生的数据量都呈指数级增长,由此产生了一系列新应用场景,传统的基于云的集中式大数据处理模式已经不能完全满足应用需求。边缘计算这种将原有的云计算中心的部分或全部计算任务迁移到数据源附近的新计算模式逐渐受到各界的广泛重视,相关企业、产业组织和开源平台也逐渐发展起来,推出了一系列边缘计算参考架构,而它们对安全都很重视。鉴于此,对已有的边缘计算参考架构中的安全部分进行分析和整理,发现其一致认为采用分层的安全措施和整体的安全监测和运营是解决边缘计算安全的有效途径。但目前还没有独立的安全框架对边缘计算安全进行系统化和完整性的论述,从而不利于边缘计算的推广和应用。因此,从安全目标、安全管理、安全技术和应用领域为制定专门的边缘计算安全框架提出了几点建议。

关键词:边缘计算;安全;参考架构;雾计算;移动边缘计算;开源项目 EdgeX
中图分类号:TP393;TP309 **文献标识码**:A

Summary and prospect of edge computing security

TAO Yaodong[1,3], *XU Wei*[2], *JI Shenglong*[3]
(1. Beijing Jiaotong University, Beijing 100000, China;
2. University of Science and Technology of China, Hefei 230031, China;
3. Qi An Xin Group, Beijing 100000, China)

Abstract: With the development of information, communication and Internet of Things technologies, the number of devices connected to the Internet and the amount of data generated have increased exponentially, resulting in a number of new application scenarios. The traditional cloud-based centralized big data processing mode cannot fully meet the needs of the new application scenarios. Edge computing is a new computing model that migrates some or all of the computing tasks of the original cloud computing center to the vicinity of the data source. It has gradually attracted widespread attention from various industries. Relevant enterprises, industrial organizations and open source platforms have published a series of reference architectures for edge computing, which these documents are highly security focused. In this paper, the existing reference architectures for edge computing are collated and analyzed, and it is found that defense-in-depth and overall security operation are the effective ways to solve the security problem of edge computing. However, there is no independent security reference architecture to systematically describe the security of edge computing, and this is not conducive to the promotion and application of edge computing. This paper gives some preliminary suggestions from the aspects of security objectives, security management, security technology and application fields.

Keywords: edge computing; security; reference architecture; fog computing; mobile edge computing; open source project EdgeX

收稿日期:2019-10-23。Received 23 Oct. 2019.

0 引言

近年来，信息通信技术迅速发展，网络、计算和存储能力呈现指数级增长，大数据、人工智能、物联网和虚拟现实等技术也逐渐发展成熟，催生出一系列新的应用和新的商业模式。云计算的应用，使得计算资源变成了一种基础服务，对信息通信产业的应用生态产生了重大的影响，从而催生了一系列新技术的应用和普及。但随着物联网技术的发展，迅速出现的海量异构的终端设备，其产生的数据量也呈指数级增长[1-2]。据相关机构预测，到 2025 年，连接到网络的无线设备数量将达到 754 亿台[3]，全球数据总量将达到 175 ZB[4]。传统的基于云的集中式大数据处理方式，已经无法完全满足万物互联条件下的实时性、隐私保护和低能耗等需求，将一部分计算功能在靠近用户和终端设备处进行处理的新的计算方式开始逐渐引起人们的重视。

边缘计算是指在网络边缘执行计算的一种新型计算模型，网络边缘是指从数据源到云计算中心路径之间的任意计算和网络资源[5]。边缘计算模型是将原有云计算中心的部分或全部计算任务迁移到数据源的附近执行，是原有云计算模型的一个补充模型，而不是替代模型[6]。边缘计算逐渐受到学术界、产业界、标准化组织和开源平台的重视，在技术、产业、标准和应用等多个方面都得到了快速的发展[7]。

为了推动边缘计算的发展，相关企业发起了相关的产业组织，特定应用领域的产业联盟和标准化组织也在其领域内部署边缘计算，并推出了一些架构建议，边缘计算相关的开源项目也逐渐发展起来[8-9]。2015 年，一些边缘计算的支持者发起成立了开放雾联盟(Open Fog Consortium，OFC)，将介于云和终端用户之间进行的边缘计算命名为“雾计算”，并于 2017 年发布了雾计算的参考架构[10]。2016 年，为促进边缘计算在各行业的数字化创新和行业应用，一些企业发起成立了边缘计算产业联盟(Edge Computing Consortium，ECC)，并与中国工业互联网产业联盟(Alliance of Industrial Internet，AII)联合发布了多个版本的边缘计算参考架构[11-13]。2014 年，欧洲电信欧洲电信标准化协会(European Telecommunications Standards Institute，ETSI)提出了移动边缘计算(Mobile Edge Computing，MEC)，认为其是 5G 的重要组成部分[14]，并发布了移动边缘计算白皮书，介绍了移动边缘计算的基本架构[15]。2018 年，美国工业互联网联盟(Industrial Internet Consortium，IIC)也发布了应用在工业物联网中的边缘计算架构[16]。开源项目 EdgeX 构建了一个开源的边缘计算架构，在其开源页面上描述了采用其架构的指南[17]。

以上参考架构都对边缘计算的安全问题进行了讨论，但到目前为止还没有专门的边缘计算安全的框架和标准，有一些学术文献已进行了一些初步的探讨，但他们仅初步分析了边缘计算的安全需求和挑战，或是仅针对某些特定技术领域进行了探讨[18-24]。为更加全面、系统和体系化地认识边缘计算安全问题，本文汇总、整理和介绍了已有边缘计算参考架构中对安全问题的描述和建议，并对其进行了简要的分析和讨论，为制定专门的边缘计算安全框架提出了一些意见和建议。

1 通用边缘计算架构中的安全问题论述

1.1 AII 和 ECC 边缘计算参考架构的安全

AII 是由我国工业和信息化部指导的，由工业、信息通信业、互联网等领域的百余家单位共同发起，于 2016 年成立的产业组织，其目标是加快我国工业互联网的发展，推进工业互联网产学研用协同发展。AII 内部设有边缘计算特设组，主要研究工业互联网边缘计算方面的问题，与边缘计算产业联盟联合发布了多个版本的边缘计算参考架构，该联盟成员已经超过1 400家。

ECC 是为拉动“政产学研用”各方资源，促进边缘计算在各行业的数字化创新和行业应用落地，引领产业健康发展，由多家公司于 2016 年联合倡议发起的一个产业组织。ECC 在《边缘计算产业联盟白皮书》中，发布了边缘计算参考架构 1.0[11]，后续又与 AII 联合发布了《边缘计算参考架构 2.0》和《边缘计算参考架构 3.0》[12-13]。另外，ECC 还与 IIC、中国自动化学会(Chinese Association of Automation，CAA)、弗劳恩霍夫开放通信系统研究所(Fraunhofer FOKUS)等一系列产业、科研和标准化组织建立了合作关系。

在 ECC 的边缘计算参考架构的更新和演化过程中，始终保持对安全问题的重视。在边缘计算参考架构 1.0 中，就在参考架构的每一层都考虑了安全问题，包括设备安全、网络安全和数据安全几方面。从 ECC 边缘计算参考架构 2.0 开始，采用多视图的方式从多个角度展示边缘计算的架构，通过跨

层功能透视图展示各层都要考虑的功能,其中就包括“安全服务”跨层功能透视图,可见其对安全问题的重视,如图 1 所示为 ECC 边缘计算参考架构 3.0 的整体结构。

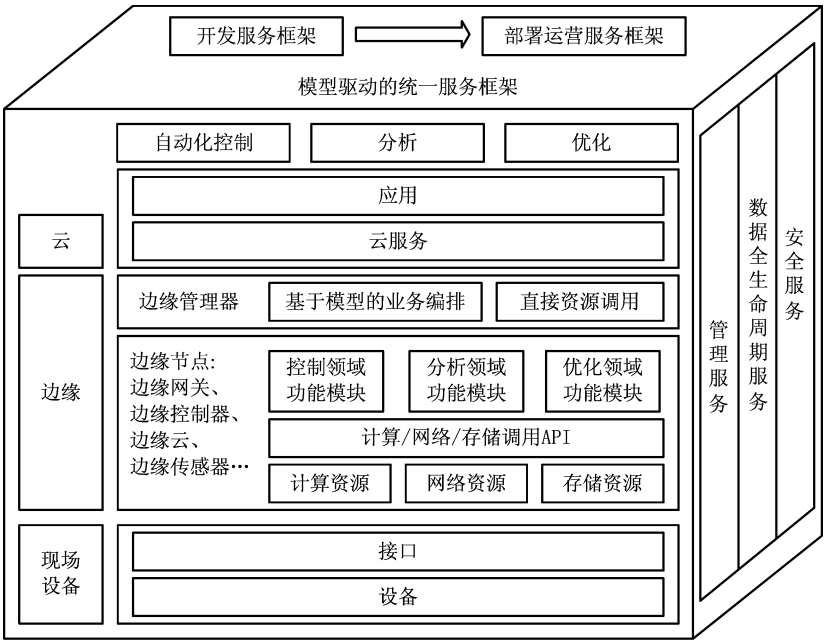

图1　ECC边缘计算参考架构3.0

ECC 边缘计算参考架构 2.0 和 3.0 还对安全服务进行了系统化的详细介绍,从边缘计算的安全需求、边缘应用场景的独特特点等角度介绍了边缘计算安全与以往信息安全之间的共性和差别,认为边缘计算具有海量、异构、资源受限、实时性和可恢复性要求高等特点。另外,提出了满足这些要求的完整的安全服务架构,如图 2 所示。

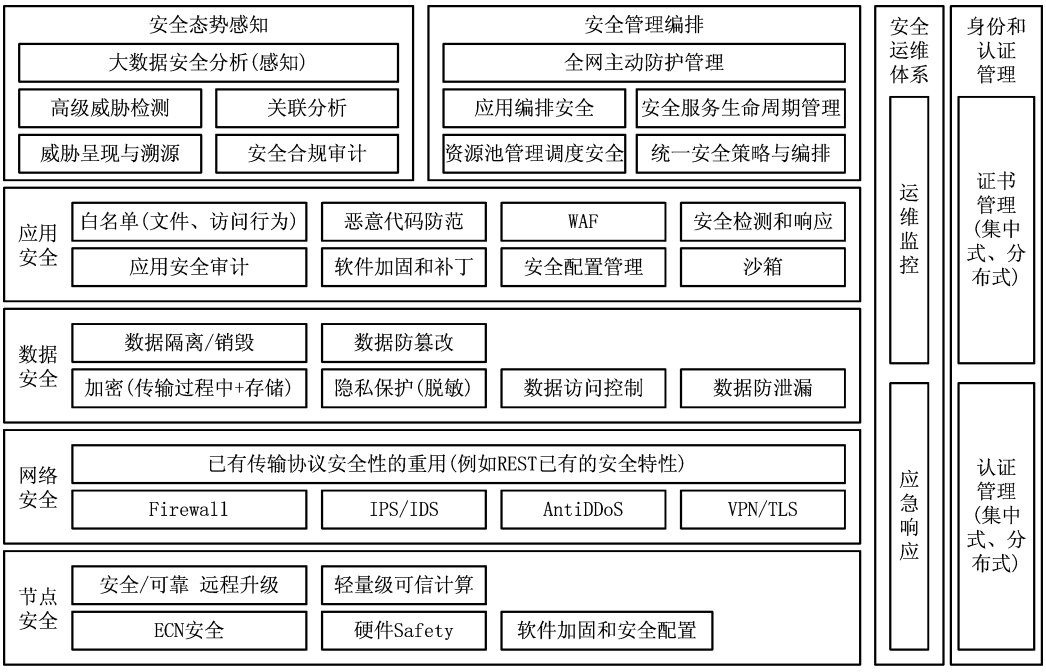

图2　ECC边缘计算参考架构3.0:安全服务

从图 2 可以看出,其安全服务架构不仅涵盖了基本的节点安全、网络安全、数据安全和应用安全等多个层次。另外,为了应对新漏洞、新威胁、新的安全管理问题以及新的网络攻击,还提出了安全态势

感知、安全管理编排、安全运维体系，以及身份和认证管理这些整体的、动态的安全技术或管理措施，在安全措施的设计过程中，也充分考虑了边缘计算的特殊需求，是一套比较体系化的安全解决方案，但限于篇幅，安全解决方案中的技术点都仅是点到为止，没有详细完整地阐述。另外，在节点安全部分，对于节点的标识解析问题也没有涉及。

1.2 OFC 雾计算参考架构的安全

开放雾联盟(OFC)是 2015 年底成立的一个产业组织，提出了“雾计算”的概念。雾计算是一种系统性的水平计算架构，其部分计算、存储、通信、控制和决策由接近用户的边缘网络设备完成。雾计算也强调是在云和用户之间的任意点进行计算，是云计算的补充[10]。从概念可以看出，雾计算与本文所说的边缘计算是完全相同的。OFC 于 2018 年 12 月已经与 IIC 合并，成为 IIC 的一部分，目前其主页已经合并到 IIC 网站[25]。

OFC 成立之初就发布了《开放雾联盟雾计算参考架构》(OpenFog Reference Architecture for fog computing，OpenFog RA)，在这个参考架构中，体系化的详细介绍了雾计算的概念、框架和应用案例[10]。OpenFog RA 由一组称为“支柱(pillar)”的核心原则指导，如图 3 所示，这八大支柱分别是：安全性、可扩展性、开放性、自治性、RAS(可靠性、可用性、可服务性)、敏捷性、层次结构和可编程性，安全性列在其中，由此可见其对安全问题的重视[10]。

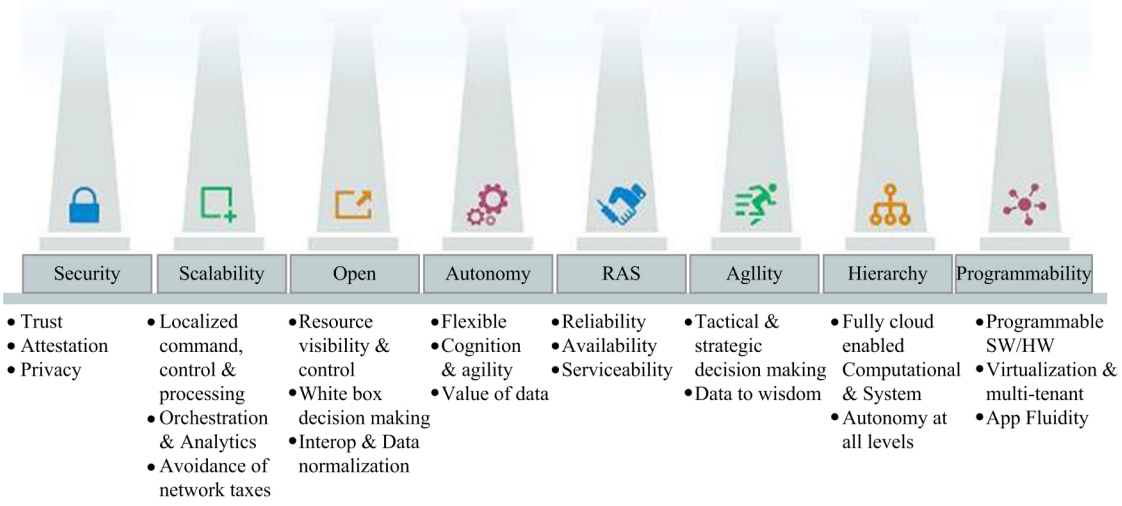

图3 OpenFog的支柱

OpenFog RA 也采用多个视图、多个视角以及跨层功能透视图相结合的方法构建系统架构，安全是跨层功能透视图之一，由此表明在系统的每个层次都要考虑安全问题，并且对系统整体部署额外的安全措施，其整体架构如图 4 所示。

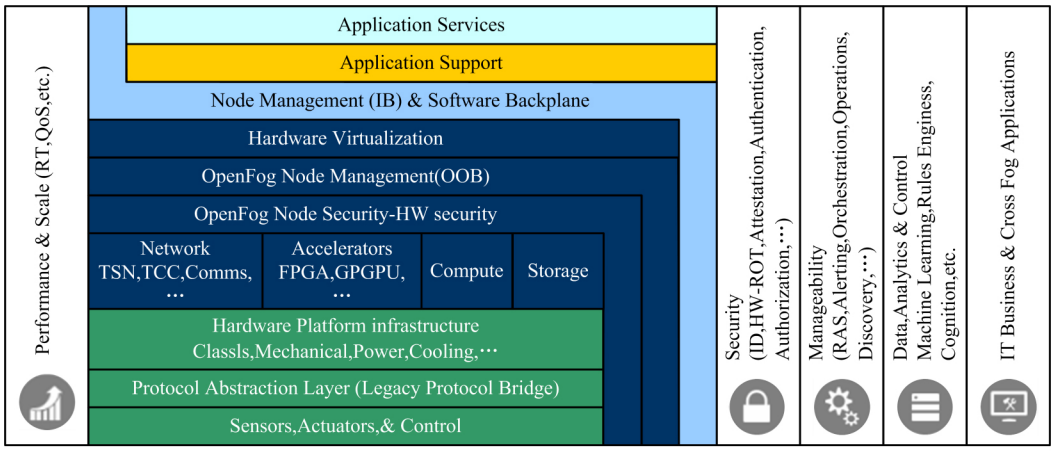

图4 OpenFog RA多视图整体架构图

在安全性透视图文字论述部分,介绍了威胁模型、CIA 三元组(机密性、完整性、可用性)、访问控制、隐私保护、可信计算和身份认证等问题。另外,还在分层介绍中对各层要实现的安全功能分别进行了介绍,如图 5 所示,具体安全功能分布在通信层、应用层、系统层和节点安全等多个层次。

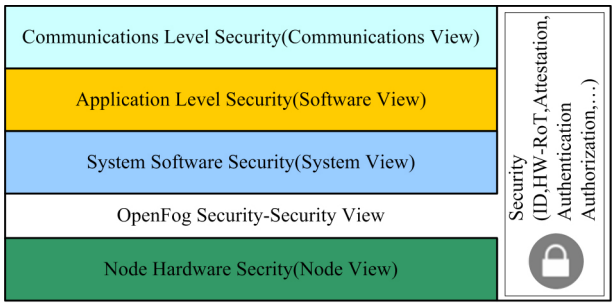

图5　OpenFog安全分层结构图

在 OpenFog RA 的附录部分进行了深入的安全分析,通过加密功能、节点安全、通信安全和数据保护 4 个方面分别对相关的技术进行了深入的介绍。但由于 OpenFog RA 相对较长(162 页),安全相关内容分散在不同章节,内容组织的系统性和条理性略显不足。

OFC 还积极参与学术交流活动,与电气和电子工程师协会(Institute of Electrical and Electronics Engineers,IEEE)合作组织了多次雾计算研讨会(Fog World Congress),吸引了很多企业和科研机构的研究者参与到雾计算研究中,构建"产学研"联动的生态系统,在会议中发表了多篇相关论文,推动了雾计算相关技术的发展,其中 OFC 安全工作组发表的一篇学术论文对雾计算的安全问题进行了更系统化的讨论[18],补充了 OpenFog RA 中安全部分的不足之处,但由于组织合并,2019 年最新一届雾计算研讨会已经更名为"开放边缘计算研讨会"(Open Edge Symposium)。

2　特定领域边缘计算架构中的安全问题论述

2.1　ETSI 移动边缘计算标准中的安全

ETSI 是由欧共体委员会 1988 年批准建立的一个非营利性的电信标准化组织,其制定的推荐性标准常被作为欧洲法规和标准的技术基础,对全球的电信标准化工作也有显著的贡献。ETSI 于 2014 年发布了《移动边缘计算介绍性技术白皮书》(Mobile-Edge Computing-Introductory Technical White Paper),该白皮书介绍了移动边缘计算 MEC 的概念和市场驱动因素,还讨论了 MEC 的需求和挑战,并提出了抽象架构图[15]。移动边缘计算是指在移动网络边缘提供 IT 服务环境和云计算能力,将网络业务下沉到更接近移动用户的无线接入网侧,旨在降低延时,实现高效网络管控和业务分发,改善用户体验。

在白皮书的"技术挑战和要求"部分单独有一小节提到了安全性的挑战和要求,认为 MEC 带来的安全挑战主要来自于将 IT 应用引入到电信领域,而电信领域的运行环境有一些特殊的合规性要求。

为应对这些安全挑战,确保 MEC 系统符合 3GPP 安全规范、运营商安全策略和当地安全监管规则,白皮书提出了应用隔离、可信计算、可信第三方应用程序和网络接口保护等多项安全措施。建议采用流量隔离、虚拟机隔离、访问控制、完整性保护和安全沙箱等技术实现应用程序隔离。建立可信计算平台,防止包括物理攻击在内的多种攻击方式;针对部署第三方应用程序带来的安全隐患,建议通过身份验证和授权、虚拟化技术、多种隔离技术相结合的方式构建可信的第三方应用程序平台,确保应用程序安全可信;网络接口保护方面,建议采用 IT 领域已经广泛应用的安全机制进行防护。

总体来说,MEC 白皮书中提到安全的部分相对较少,简单介绍了 MEC 的安全挑战和应对方式,且缺乏体系化论述。而且 MEC 概念本身也在发展过程中发生了变化,原来的"移动边缘计算"目前已经改称为"多接入边缘计算"(Multi-access Edge Computing, MEC),多接入边缘计算是指在网络边缘为应用研发商和内容提供商提供 IT 服务环境和云计算能力,该环境为应用提供了超低延时、高带宽、实时接入等特性能力。在概念演进后安全需求也会有所改变,相关内容可能会在 ETSI 的后续研究报告中呈现。

2.2　IIC 的工业物联网边缘计算的安全

美国工业互联网联盟(IIC)是 2014 年由多家跨国公司和科研机构发起成立的一个产业组织,旨在实现工业互联网的标准化,推动工业互联网的发展,其先后发布了一些列白皮书,如《工业互联网参考架构》(The Industrial Internet of Things Volume G1: Reference Architecture, IIRA)[26]、《工业互联网安全框架》(Industrial Internet Security Framework, IISF)[27]等。

IIC 对边缘计算也逐渐关注并重视起来,于

2018 年发布了《IIoT 中的边缘计算简介》(Introduction to Edge Computing in IIoT)白皮书[16]。在白皮书中,通过三层架构和五个跨层功能透视图的方式介绍了 IIoT 中的边缘计算。如图 6 所示,三层架构是指 IIRA 中描述的边缘、平台和企业层,跨层功能透视图是指某些功能要跨越每个层级才能完成的独立功能,包括数据管理、连接通信、策略编排、工业分析和安全。白皮书还针对哪儿是边缘、为什么要在边缘侧进行计算和 IIoT 中的边缘计算有何特点等问题展开了讨论。

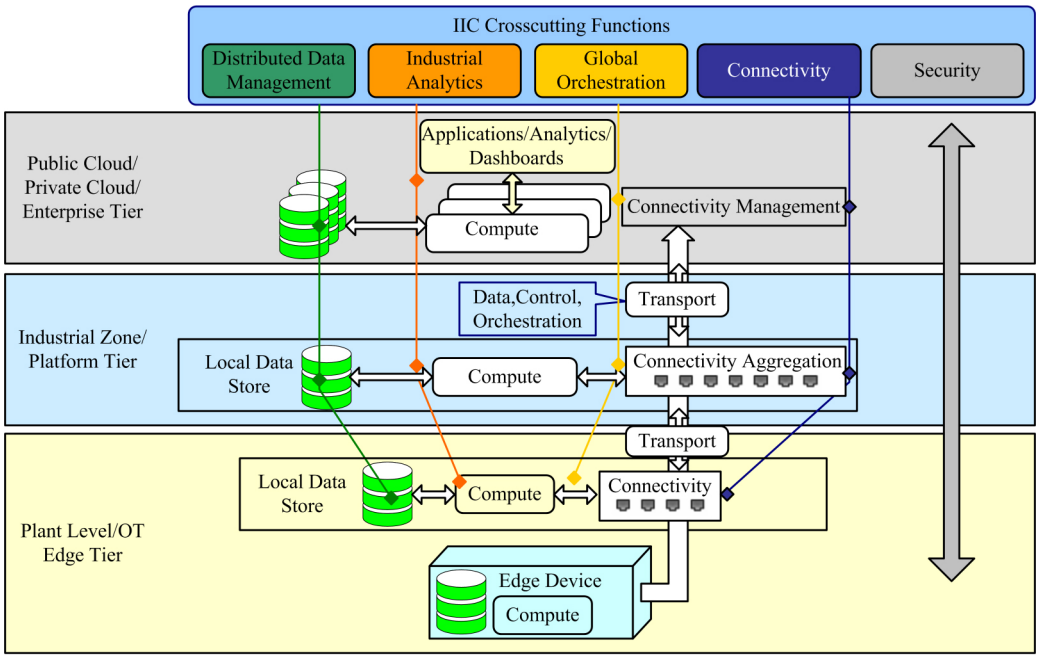

图6 IIoT中的边缘计算架构的跨层功能

如图 6 所示,其将安全作为跨层功能透视图的一部分,可见在 IIoT 边缘计算架构的设计过程中充分重视安全问题,将安全作为基本架构的重要组成部分,跨越从边缘层、平台层和企业层的整个体系结构,说明每一层都应当单独考虑安全问题,整体还要额外考虑安全问题。在白皮书中单独有一章讨论了 IIoT 边缘计算的安全问题,认为在工业领域增加更多的信息组件和通信连接引入了新的攻击向量,需要采用创新的方式进行安全监测和防护。IIoT 构建过程中主要参考 IISF 的端到端安全框架,但在采用边缘计算架构时,还应考虑设备和网络的内生安全、对计算和网络节点进行安全监测、及时打补丁保持版本更新、攻击隔离和攻击后可恢复性等问题。

综上所述,《IIoT 边缘计算白皮书》对安全问题也很重视,在体系架构中有明显的体现,但因为该组织还存在 IISF 这样的系统化安全框架,所以仅介绍了 IIoT 中边缘计算的特殊要求,相关论述相对较少,仅涉及几个特定的问题,没有形成体系化的完整安全框架。

3 边缘计算开源项目中的安全问题论述

EdgeX 是由 Linux 基金会托管的,与供应商无关的一个开源项目,为 IoT 边缘计算构建了一个通用的开放框架。EdgeX 作为物联网边缘计算的统一开放平台,实现各组件即插即用的生态系统,能够统一市场并加速 IoT 解决方案的部署。如图 7 所示,EdgeX 的基础是一个松耦合的分层物联网体系架构,在架构的侧面有两个横跨多层模块,分别是安全和管理,建议在架构的所有层级都应当考虑安全和管理这两个问题。

EdgeX 项目是一个开源项目,其介绍文档中有一个一级目录介绍安全,其中包括报告安全问题、安全部署(WIP)、安全威胁和已知安全问题,由于项目还没有完成,这些文档目前也还没有撰写完成。威胁模型部分是一个在 2019 年北美开源峰会上的演讲文档,该文档介绍了通过 STRIDE 威胁模型对 EdgeX 进行威胁建模的过程,多维度分析了 EdgeX 的资产和威胁,并介绍了通过 API 网关安全模式减少攻击面、预防 DoS 攻击和认证授权的风险缓解措施[28]。

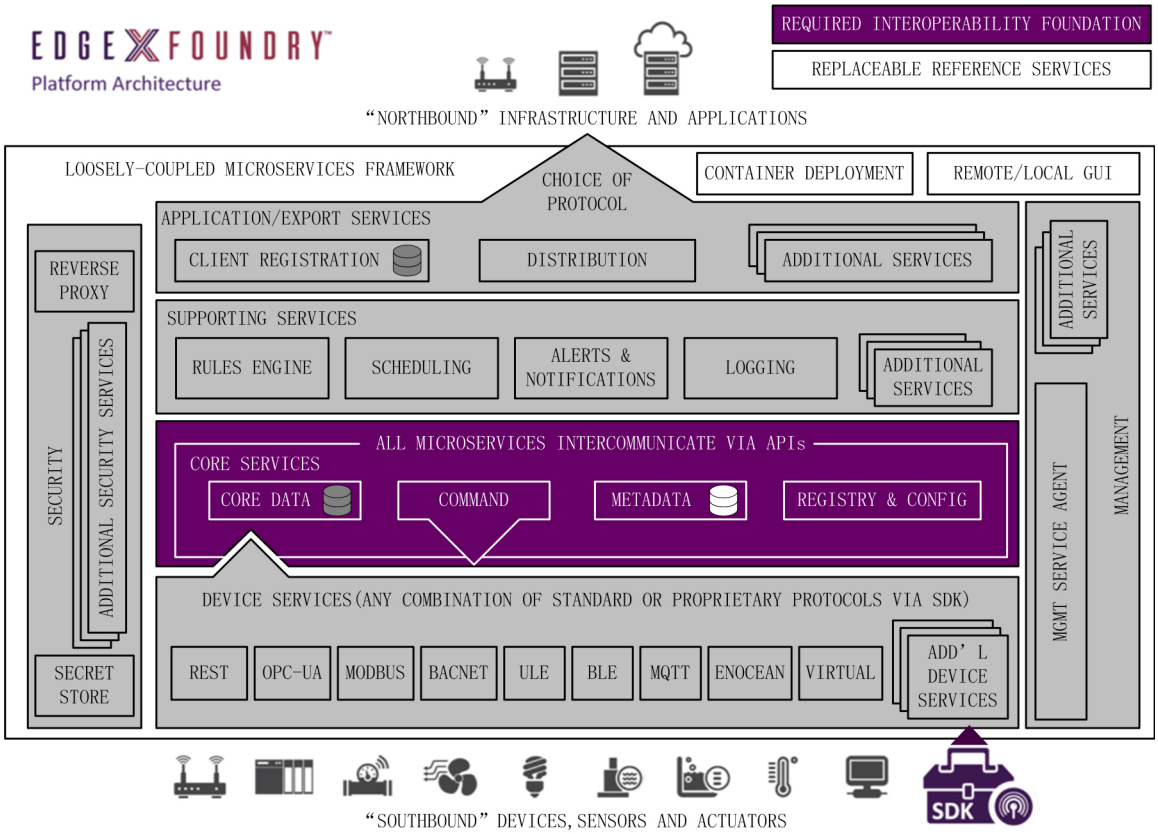

图7　EdgeX平台架构图

可以看出,EdgeX 架构中虽然重视安全问题,但尚未对安全问题进行全面和系统的讨论,在后续的开发过程中会逐渐丰富起来。

4　讨论与建议

根据对多种边缘计算架构中安全问题论述的汇总与分析可以看出,边缘计算的海量、异构、资源受限、实时性和可恢复性要求高等特点带来了一系列安全挑战,为了应对这些安全需求和挑战,相关的参考架构都采取了一系列的技术和管理应对措施。

通用的边缘计算参考架构一般会比较全面地讨论安全问题,而特定应用领域的边缘计算架构一般仅讨论其特殊的安全需求和挑战,开源项目中的安全部分则仅涉及与其项目相关的内容。在这些边缘计算参考架构中,一般将安全定义为跨层功能透视图,以此表示边缘计算的每个层级都应该考虑安全问题,还应该有整体的安全措施保证边缘计算系统的整体安全。虽然使用的名词不同,但 ECC 和 OFC 都提到了节点安全、网络安全、应用安全和数据安全等部分,可见这是边缘计算需要重点考虑的问题。整体安全保障措施一般包括安全监控和安全管理,用来应对未知漏洞和整体威胁。虽然边缘计算有一些共性的安全需求,但特定应用领域的边缘计算的安全挑战和需求具有较大的差异。

虽然上文提到的边缘计算参考架构都对安全问题很重视,但是到目前为止还没有独立的安全参考框架对边缘计算的安全问题进行系统性和完整性的阐述,业界目前亟待解决这一问题。本文基于已有论述的汇总分析,对于制定独立的边缘计算安全参考框架提出以下建议:

(1)安全目标方面　应当考虑将可信任作为一个安全目标。传统的信息安全一般考虑保密性、完整性和可用性三元组(简称 CIA)。边缘计算场景下,海量设备分布式部署,极大地增加了设备损坏、丢失、篡改和仿冒的风险,因此除了需要保证传统的 CIA 安全三元组以外,还应当考虑系统内设备和组件的可信任问题。保证设备可信任,可以通过硬件、固件和软件应用相结合的方式通过可信计算技术保证信任链的传递形成可信执行环境。为保证可信任,还需要构建标识解析体系,并构建标识解析体系的安全防护措施。可信计算的内容在 ECC 和 OFC 的参考架构中有相关的描述,但没有将可信任性上

升到安全目标的层面，也没有涵盖标识解析体系的内容。

(2)安全管理方面　可以通过全生命周期安全管理的模式确保边缘计算安全。在边缘计算架构下，涉及到平台开发方、平台运营方、软硬件组件供应商、集成商、应用开发者和最终用户等多方参与，系统复杂度的逐渐提高，安全管理的难度也逐渐增加。为有效地实现安全管理，需要多方协调，任何一环出现安全问题都将影响整个系统正常运转，采用安全生命周期管理模式是一个行之有效的解决方法。在边缘计算的全生命周期全程考虑安全，设立关键检查点，通过安全开发管理、代码审计、脆弱性评估、渗透测试、安全运维和事件响应与恢复等安全措施，及时发现问题和解决问题，从而有利于厘清多方关系并确保边缘计算体系的安全运行。

(3)安全技术方面　可以通过边云协同的方式提高安全能力。边缘计算有其自身的优点，能补充云计算模式的不足，但云计算本身也有很多优势。在安全方面的威胁情报、态势感知、安全运营、安全管理与编排和标识解析体系等技术领域，云计算的集中式大数据处理能力有很大的优势，如果能将边云协同的模式这些优势在边缘计算安全中发挥出来，将可以有效提高边缘计算的安全能力。

(4)应用领域方面　可以通过分场景讨论的方式提高针对性。边缘计算的应用领域很广，从上文的描述可以看出，边缘计算目前已经广泛应用在物联网、工业互联网和电信运营商等多个领域，以后应用领域未来还会扩展，不同应用领域差异性很大，采用统一的安全框架和标准很难完全满足多种场景，可以通过各领域分别制定安全框架，或通用安全框架分领域进行讨论的方式提高针对性和适用性。

5　结束语

本文收集了已有边缘计算参考架构中对安全问题的论述，并对其进行了分析和整理。从中可以看出，边缘计算的海量、异构、资源受限、实时性和可恢复性要求高等特点带来了一些新的安全挑战。为应对这些安全挑战，已有架构中的安全论述已经提出了一些解决方案，普遍认为采用分层的安全措施与整体的安全监测运营相结合的方法是解决安全问题的有效途径。但到目前为止，还没有独立的安全框架对边缘计算安全问题进行系统性和完整性的论述。本文提出了将可信任性作为安全目标、采用全生命周期安全管理模式、通过边云协同提高安全能力和分场景讨论安全问题等几点建议。如果能够根据以上建议构建单独的边缘安全框架，将会对边缘计算的健康发展起到积极的促进作用。

另外，边缘计算基础技术尚处于发展成熟期，逐渐提出了一些适用于边缘计算的新技术，如模型压缩和分割[20-30]、边缘缓存[31]、联邦学习[32]和迁移学习[33]等，也将缓解边缘计算的安全威胁。

参考文献：

[1] CAICT. White paper on Internet of things[R]. Beijing: China Academy of Information and Communications Technology(CAICT), 2018: 47(in Chinese). [中国信息通信研究院. 物联网白皮书[R]. 北京：中国信息通信研究院(CAICT), 2018: 47.]

[2] XU Wei, TAO Yaodong, GUAN Xin. The landscape of industrial control systems(ICS) devices on the internet[C]//Proceedings of 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). Washingtong, D. C., USA: IEEE, 2018: 1-8.

[3] IHS Markit. IoT platforms: enabling the Internet of things [EB/OL]. [2019-09-18]. https://technology.ihs.com/576272?utm_campaign=PR_iot-platforms-enabling-the-internet-of-things-001&utm_medium=press_release&utm_source=Newsroom.

[4] IDC. The digitization of the world—From edge to core[R]. Beijing: International Data Corporation (IDC), 2019 (in Chinese). [IDC. 数字化世界——从边缘到核心[R]. 北京：国际数据公司(IDC), 2019.]

[5] SHI Weisong, SUN Hui, CAO Jie, et al. Edge computing—an emerging computing model for the internet of everything era [J]. Journal of Computer Research and Development, 2017, 54(5): 907-924(in Chinese). [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.]

[6] SHI W, CAO J, ZHANG Q, et al. Edge computing: vision and challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.

[7] SHI Weisong, ZHANG Xingzhou, WANG Yifan, et al. Edge computing: state-of-the-art and future directions[J]. Journal of Computer Research and Development, 2019, 56(1): 69-89(in Chinese). [施巍松，张星洲，王一帆，等. 边缘计算：现状与展望[J]. 计算机研究与发展, 2019, 56(1): 69-89.]

[8] LÜ Huazhang, CHEN Dan, FAN Bin, et al. Standardization progress and case analysis of edge computing[J]. Journal of Computer Research and Development, 2018, 55(3): 487-511(in Chinese). [吕华章，陈　丹，范　斌，等. 边缘计算标准化进展与案例分析[J]. 计算机研究与发展, 2018, 55(3): 487-511.]

[9] LIN Bo, ZHANG Huimin. Analysis and research based on edge computing platform[J]. Computer and Information Technology, 2019, 27(4): 21-24, 47(in Chinese). [林　博，张惠民. 基于边缘计算平台的分析与研究[J]. 电脑与信息技术, 2019, 27(4): 21-24, 47.]

[10] OpenFog. Reference architecture for fog computing [R].

Princeton, N. J., USA: OpenFog Consortium, 2017: 162.

[11] ECC. White paper of Edge Computing Consortium[R]. Beijing: Edge Computing Consortium (ECC), 2016: 23 (in Chinese). [边缘计算产业联盟. 边缘计算产业联盟白皮书[R]. 北京:边缘计算产业联盟(ECC),2016:23.]

[12] ECC/AII. Edge computing reference architectures 2.0[R]. Beijing: Edge Computing Consortium (ECC)/Alliance of Industrial Internet (AII), 2017: 50 (in Chinese). [边缘计算产业联盟(ECC)/工业互联网产业联盟(AII). 边缘计算参考架构 2.0[R]. 北京:边缘计算产业联盟(ECC)/工业互联网产业联盟(AII),2017:50.]

[13] ECC/AII. Edge computing reference architectures 3.0[R]. Beijing: Edge Computing Consortium (ECC)/Alliance of Industrial Internet (AII), 2018: 42 (in Chinese). [边缘计算产业联盟(ECC)/工业互联网产业联盟(AII). 边缘计算参考架构 3.0[R]. 北京:边缘计算产业联盟(ECC)、工业互联网产业联盟(AII),2018:42.]

[14] HU Y C, PATEL M, SABELLA D, et al. Mobile edge computing—A key technology towards 5G[J]. ETSI white paper, 2015, 11(11): 1-16.

[15] PATEL M, NAUGHTON B, CHAN C, et al. Mobile-edge computing introductory technical white paper[R]. London, UK: European Telecommunications Standards Institute (ETSI), 2014: 36.

[16] IIC. Introduction to edge computing in IIoT[R]. Needham, Mass., USA: Industrial Internet Consortium (IIC), 2018: 19.

[17] EdgeX Foundry. EdgeX foundry project Wiki[EB/OL]. [2019-09-13]. https://wiki.edgexfoundry.org/display/FA/EdgeX+Foundry+Project+Wiki.

[18] MUKHERJEE M, MATAM R, SHU L, et al. Security and privacy in fog computing: Challenges[J]. IEEE Access, 2017, 5: 19293-19304.

[19] 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.

[20] YI S, QIN Z, LI Q. Security and privacy issues of fog computing: A survey[C]//Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications. Beilin, Germany: Springer-Verlag, 2015: 685-695.

[21] ZHANG Jiale, ZHAO Yanchao, CHEN Bing, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal on Communications, 2018, 39(3): 1-21 (in Chinese). [张佳乐,赵彦超,陈　兵,等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报,2018,39(3):1-21.]

[22] MA Lichuan, PEI Qingqi, XIAO Huizi. Security requirements and challenges in edge computing for internet of everything[J]. ZTE Technology Journal, 2019, 25(3): 37-42 (in Chinese). [马立川,裴庆祺,肖慧子. 万物互联背景下的边缘计算安全需求与挑战[J]. 中兴通讯技术,2019,25(3):37-42.]

[23] NING Zhenyu, ZHANG Fengwei, SHI Weisong. A study of using TEE on edge computing[J]. Journal of Computer Research and Development, 2019, 56(7): 1441-1453 (in Chinese). [宁振宇,张锋巍,施巍松. 基于边缘计算的可信执行环境研究[J]. 计算机研究与发展,2019,56(7):1441-1453.]

[24] LING Jie, CHEN Jiahui, LUO Yu, et al. A survey on the security technology of edge computing[J]. Big Data Research, 2019, 5(2): 34-52 (in Chinese). [凌　捷,陈家辉,罗　玉,等. 边缘计算安全技术综述[J]. 大数据,2019,5(2):34-52.]

[25] Industrial Internet Consortium. The industrial Internet consortium and OpenFog consortium join forces[EB/OL]. [2019-09-13]. https://www.iiconsortium.org/press-room/12-18-18.htm.

[26] IIC. The Industrial Internet of things volume G1: reference architecture[R]. Needham, Mass., USA: Industrial Internet Consortium (IIC), 2017: 58.

[27] IIC. Industrial Internet of things volume G4: security framework[R]. Needham, Mass., USA: Industrial Internet Consortium (IIC), 2016: 173.

[28] Open Source Summit. An agile approach to threat modeling for securing EdgeX foundry[EB/OL]. [2019-09-13]. https://ossna19.sched.com/event/PUUx.

[29] HAN Song, MAO Huizi, DALLY W J. Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding[EB/OL]. (2016-02-15) [2019-09-13]. http://arxiv.org/pdf/151000149.pdf.

[30] KANG Y, HAUSWALD J, GAO C, et al. Neurosurgeon: collaborative intelligence between the cloud and mobile edge [C]//Proceedings of ACM SIGARCH Computer Architecture News. New York, N. Y., USA: 2017: 615-629.

[31] DROLIA U, GUO K, TAN J, et al. Cachier: Edge-caching for recognition applications[C]// Proceeding of the 37th IEEE International Conference on Distributed Computing Systems (ICDCS). Washingtong, D. C., USA: IEEE, 2017: 276-286.

[32] FERRAG M A, DERHAB A, MAGLARAS L, et al. Privacy-preserving schemes for fog-based IoT applications: threat models, solutions, and challenges[C]//Proceedings of 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT). Washington, D. C., USA: IEEE, 2018: 37-42.

[33] SHARMA R, BIOOKAGHAZADEH S, Li B, et al. Are existing knowledge transfer techniques effective for deep learning with edge devices? [C]//Proceedings of 2018 IEEE International Conference on Edge Computing (EDGE). Washington, D. C., USA: IEEE, 2018: 42-49.

作者简介:

陶耀东(1981－),男,北京交通大学工业互联网安全研究中心主任,教授,AII 安全组主席,ECC 安全组主席,研究方向:工业互联网安全、边缘计算安全,E-mail:ydtao@bjtu.edu.cn;

徐　伟(1983－),男,中国科技大学博士研究生,工程师,研究方向:工业互联网安全、边缘计算安全,E-mail:xu5ei@mail.ustc.edu.cn;

纪胜龙(1980－),男,工程师,研究方向:工业互联网安全、边缘计算安全,E-mail:jishenglong@qianxin.com。