边缘计算安全与隐私保护研究进展

沈传年
(国家计算机网络应急技术处理协调中心上海分中心，上海 201315)

摘　要： 物联网、5G 等信息技术的快速发展加速了万物互联时代的到来，网络边缘设备的爆发式增长产生了海量级边缘数据，传统云计算模型的集中式大数据处理已无法满足对边缘设备海量数据的高效处理。边缘计算作为一种新型计算模型，在更靠近用户的网络边缘侧就近提供服务，减缓了网络负载，增强了响应能力，但同时由于边缘环境的开放性、多源异构性、边缘节点资源受限等特性，使得边缘计算的安全与隐私保护面临诸多挑战。首先从安全需求出发，围绕身份认证、通信安全协议、入侵检测以及隐私保护等关键技术，系统阐述和分析了边缘计算安全与隐私保护领域的国内外研究成果，最后提出了未来可能的研究方向。

关键词： 边缘计算；身份认证；入侵检测；隐私保护
中图分类号： TP309　　**文献标识码：** A　　**DOI：** 10.20044/j.csdg.2097-1788.2022.02.007
引用格式： 沈传年. 边缘计算安全与隐私保护研究进展[J]. 网络安全与数据治理，2022，41(2)：41-48.

Research progress of edge computing security and privacy-preserving

Shen Chuannian
(National Computer Network Emergency Response Technical Team/Coordination Center of China@Shanghai, Shanghai 201315, China)

Abstract: The rapid development of information technologies such as the Internet of Things and 5G accelerates the arrival of the era of the Internet of Everything, the explosive growth of network edge devices has produced massive edge data, the centralized big data processing of the traditional cloud computing model has been unable to meet the efficient processing of massive data of edge devices, therefore, edge computing comes into being at the right time. As a new computing model, edge computing provides services closer to the user's network edge side, which reduces the network load and enhances the response ability. However, due to the openness and multi-source heterogeneity of the edge environment, the resources of edge nodes restriction and other characteristics make the security and privacy-preserving of edge computing faces many challenges. Firstly, the basic concept of edge computing is introduced, and then from the perspective of security requirements, focusing on the key technologies such as identity authentication, communication security protocol, intrusion detection and privacy-preserving, the research achievements in the field of edge computing security and privacy-preserving at home and abroad are systematically described and analyzed. Finally, the possible research directions in the future are proposed.

Key words: edge computing; identity authentication; intrusion detection; privacy-preserving

0 引言

近年来，随着物联网、大数据、人工智能、区块链、5G 等信息技术的快速发展，万物互联趋势急速加剧，增强现实/虚拟现实、智能家居、智慧城市、远程医疗、无人驾驶等新型业务模式不断涌现，已广泛应用于日常生活中并带来了极大的便利。网络技术和应用服务的进一步发展使网络边缘设备的连接数量呈现爆发式增长态势，与之相伴的是网络边缘设备所产生的海量级数据。根据 Gartner 的数据预测，到 2022 年，超过 50%的企业数据将在网络边缘侧产生和处理。据国际数据中心(IDC)数据时代报告《世界的数字化：从边缘到核心》预测，到 2025 年全球将产生 175 ZB(泽字节)的数据(1 ZB 相当于 1 万亿 GB)，其中全球数十亿台边缘设备将产生

90 ZB 以上的数据。

目前,海量数据的存储和处理主要依赖于集中式的云计算[1]模式,即将所有数据通过网络传输到远程云端数据中心,利用云端数据中心强大的计算能力集中式地解决计算和存储问题。但随着物联网和 5G 时代的到来,以及云计算应用的不断激增,越来越多的应用场景中需要计算庞大的数据并且能够得到实时的反馈,而目前网络带宽的增长速度远落后于数据量的增长速度,同时复杂的网络环境让网络时延难以显著优化,因此,传统云计算模式已经无法满足网络边缘侧“大连接、低时延、高带宽”的资源需求,难以实时高效地支撑起基于万物互联的应用服务,其暴露出的种种不足,主要表现在三个方面:

(1)带宽和资源消耗问题。网络边缘设备产生的海量数据使云计算的网络带宽、计算资源以及存储资源变得日趋紧张,给以中心服务器为节点的云计算造成更大的数据瓶颈;

(2)数据处理的实时性问题。云计算是在远程数据中心集中进行数据处理,由于数据需要在边缘设备和云数据中心之间进行异地长距离传输,必然会产生较高的网络时延;

(3)用户隐私保护问题。云计算模式下,所有用户数据都需要上传并存储在云数据中心。云数据中心由于无法对用户数据的访问和使用进行精细控制,容易导致用户隐私数据遭受恶易攻击、泄露和非法利用等风险[2]。

因此,在网络终端边缘侧处理数据的模式,即边缘计算[3]应时而生,并迅速成为近年来的研究热点[4]。

1 边缘计算概述

1.1 边缘计算概念

边缘计算的概念最早可以追溯至 1998 年 Akamai 公司提出的内容分发网络技术 (CDN),强调内容的备份和缓存,而边缘计算的基本思想则是功能缓存[5]。施巍松教授定义边缘计算为在网络边缘执行计算的一种新型计算模型[6],对象包括来自于云服务的下行数据和来自万物互联服务的上行数据,而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。ISO 定义边缘计算为“将数据和任务在靠近数据源头的网络边缘侧进行计算和执行的一种新型服务模型”[7]。边缘计算产业联盟定义边缘计算为“在靠近物或数据源头的网络边缘侧,融合网络、计算、存储、应用核心能力的开放平台”。尽管表述各有差异,但在边缘计算的核心概念上基本形成了共识,即边缘计算将云计算的能力拓展至距离网络终端更近的边缘侧,计算更靠近数据源头,更贴近用户,无需上传云端,从而有效减缓了网络带宽负载,增强了服务响应能力。

1.2 边缘计算参考架构

边缘计算产业联盟和工业互联网产业联盟于 2018 年 11 月联合提出了边缘计算参考架构 3.0[8],如图 1 所示。从架构的横向层次来看,上侧部分是模型驱动的统一服务框架,可实现开发服务和部署运营服务;下侧部分分为云、边缘和现场设备三层,边缘层位于云和现场设备之间,向上对接云端,向下可支持各种现场设备的接入。边缘层又包括边缘管理器和边缘节点两个层次,边缘管理器的主要功能是以软件的形式对边缘节点进行统一管理,边缘节点是承载边缘计算业务的核心,包括边缘网关、边缘控制器、边缘云以及边缘传感器等。边缘节点一般具有计算、网络和存储资源,边缘节点对于以上资源的使用,一方面边缘管理器可以直接通过所提供的 API 进行资源调用;另一方面,可以将资源按控制、分析、优化不同功能领域封装成功能模块,边缘管理器通过基于模型的业务编排方式调用功能模块,实现边缘计算业务的开发服务。从架构的纵向层次来看,通过管理服务、数据全生命周期服务、安全服务,实现全流程、全生命周期的服务。

2 边缘计算安全需求分析

2.1 边缘计算安全模型

边缘计算由于是分布式部署,相较于云计算,接入设备具有开放性、复杂性和多源异构性,边缘节点计算能力和存储资源有限。由于边缘计算自身的特性,传统云计算环境下的安全机制无法直接应用于边缘计算,因此,如何设计基于边缘计算的安全与隐私保护方案已成为边缘计算的研究重点。

针对边缘计算不同层级差异化的安全防护需求,边缘计算安全模型[9](如图 2 所示)聚焦基础设施安全、网络安全、数据安全、应用安全四个层级,细化分解了边缘计算的安全问题,指出应在每一层中解决安全和隐私问题。

2.2 边缘计算安全需求

根据边缘计算安全模型视图,边缘计算安全需求主要分为基础设施安全、网络安全、数据安全、应

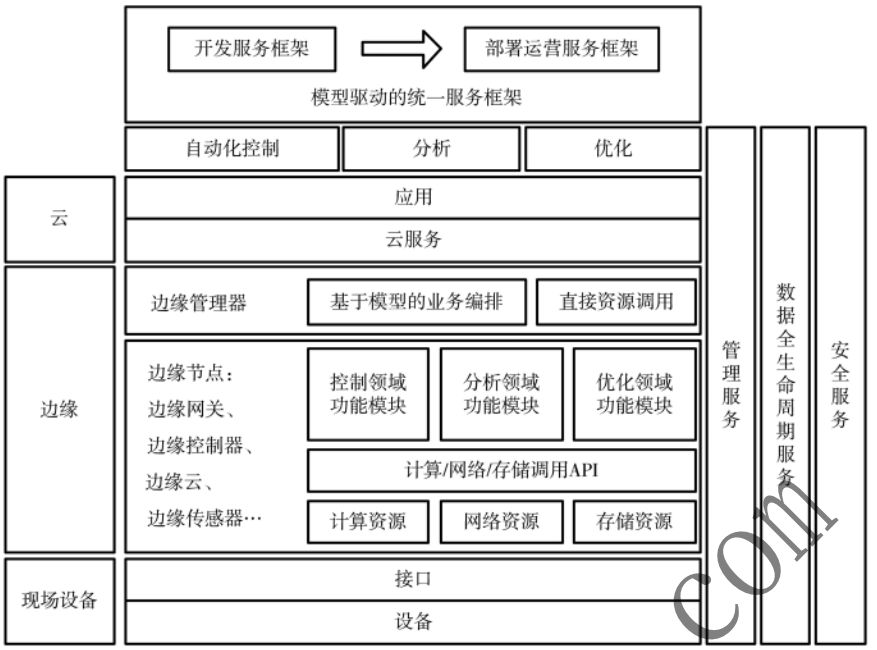

图 1 边缘计算参考架构 3.0

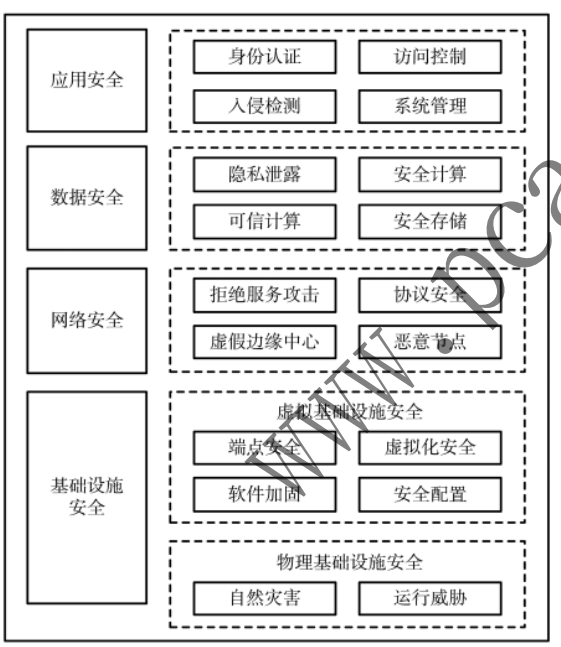

图 2 边缘计算安全模型

用安全 4 个方面的需求。

2.2.1 基础设施安全

边缘基础设施为整个边缘计算节点提供软硬件基础，边缘基础设施安全为上层应用的可靠运行提供基本保障，分为物理基础设施安全和虚拟基础设施安全。物理基础设施安全风险是指边缘基础设施由于靠近数据源头而遭受自然界中不可抗力(如地震、台风、水灾等)的影响，以及由于人为操作失误或运行保障不力(如电力能源供应、设备损耗等)导致的基础设施设备损坏、服务中断、数据丢失、性能下降等安全风险。而虚拟基础设施安全需要保证边缘基础设施在启动、运行、操作等过程中的计算环境的安全可信，建立涵盖端点安全、虚拟化安全、软件加固、安全配置等的信任链条。

2.2.2 网络安全

边缘计算模型作为新型计算模型，通过网络层实现海量终端设备与边缘节点的数据传输，因其联网设备的规模和产生的数据量极其庞大，网络边缘计算环境高度动态，且相较云计算数据中心的中心化防护，边缘节点自身的防御能力有限，不可避免带来边缘计算场景下新的网络安全风险挑战，如拒绝服务攻击[10]、通信协议安全[11]、虚假边缘中心、恶意节点等。现有网络安全防护方法并不能完全适用于边缘计算架构，边缘网络安全防护需要设计适合于边缘计算场景的纵深防御体系，包括通信安全协议、网络监测、网络防护等，从内到外保障边缘网络安全，确保网络正常可靠运行、服务不中断。

2.2.3 数据安全

由于边缘计算是在位于靠近数据源的网络边缘侧提供数据的计算与存储能力，相较于位于核心网络中的云计算数据中心，虽然在一定程度上降低

了由数据在网络中长距离传输而导致的隐私泄露风险,但是由于边缘节点可以直接主动收集获取用户的大量第一手数据,包括个人账户信息、社交信息、位置信息以及行为信息等,容易造成隐私数据被动泄露或遭受中间人攻击等潜在风险。因此,如何能够保证在安全使用边缘数据计算和存储服务的同时,又不泄露用户隐私数据信息,确保数据的机密性、可用性和完整性,成为边缘计算数据安全的关键需求。

2.2.4 应用安全

边缘计算场景下,越来越多的应用服务从云计算中心迁移到网络边缘侧,以确保应用服务响应的实时性和可靠性。边缘应用安全是满足第三方边缘应用开发和运行过程中的基本安全,以及防止恶意应用对边缘计算平台及其他应用服务产生的安全影响。边缘计算不仅与其他计算模式存在共性应用安全问题,还由于行业领域差异化需求、应用服务提供商不同、多种安全域和接入网络共存而导致的特有应用安全问题。如何对用户身份进行管理,实现资源的授权访问,对系统内未授权的网络异常行为进行检测等,便是在边缘计算环境下保证应用安全的重要需求。

3 边缘计算安全与隐私保护关键技术

边缘计算具有广泛的市场前景和应用范围,边缘计算兴起的同时也将带来新的安全挑战,一方面,由于边缘计算更靠近用户侧,异构、复杂、多样的环境和服务使得安全问题得不到保证;另一方面,边缘计算中的隐私保护也面临着各种各样的安全威胁。而目前,业界针对边缘计算安全和隐私保护的技术研究尚处于探索阶段,大多数的研究成果都集中在云计算、雾计算等计算模式下,因此,如何有效借鉴其他计算模式的安全与隐私保护方案,并与边缘计算分布式、大连接、低时延、异构性、动态性、资源受限等特性相结合,设计出一套适合边缘计算环境的安全机制来保证系统的完整性、机密性和可靠性是当前边缘计算安全领域研究的方向,本节从用户认证技术、通信安全协议、入侵检测技术以及隐私保护技术4个方面,参考其他计算环境下的重要研究成果进行综述,并给出了研究建议。

3.1 身份认证技术

在边缘计算中,当终端设备首次向边缘节点申请服务时,需要完成初始化认证以确保只有合法设备接入边缘节点。由于边缘节点计算和存储资源有限,而传统的数字签名安全认证方法需要较高的计算能力和资源消耗,这些方法已经不再适用于边缘计算中的安全认证,本部分内容将从单一身份认证、联合身份认证、切换身份认证3个方面对各计算环境下的身份认证技术进行介绍和分析。

3.1.1 单一身份认证

单一身份认证是指在边缘计算单一信任域内,终端用户通过授权中心的安全认证获得访问资源权限的过程。Touceda等[12]提出了一种基于属性证书的结构化P2P网络授权方案,该属性证书将系统内用户的权限与用户身份表示为一个公钥证书,指出点对点计算可以相互认证而不需要连接到中央认证服务器。Echeverría等[13]提出了一种适用于断开连接环境的可信身份认证方案,它将基于身份的加密与无需可信第三方的安全密钥交换机制相结合,可应用于两个或多个计算节点之间的任何形式的可信通信。

3.1.2 联合身份认证

联合身份认证是在不同服务商的身份信息库间建立关联,使用户只需在使用某个边缘服务时认证一次,就可以跨域访问所有相互信任的边缘服务。基于公钥基础设施(Public Key Infrastructure,PKI)的联合身份认证技术是目前广泛被采纳的一种联合身份认证方案,朱智强[14]提出了一种基于公钥基础设施和基于身份的密码技术(Identity-Based Cryptography,IBC)组合的面向混合云的跨云认证模型,PKI只签发云一级证书,通过PKI建立云间的信任关系,IBC通过使用PKI证书实现不同IBC域间的跨云操作,且能够支持大范围的操作。Ibrahim[15]提出了一种安全且高效的认证方案,该方案不需要使用任何PKI,用户只需要在注册阶段存储一个主密钥,使用此主密钥,用户便能够与云服务商管理的任何雾服务器进行相互认证,即使所有雾服务器遭受攻击,用户主密钥由于具有足够的长度可以防止被暴力破解。

3.1.3 切换身份认证

边缘计算中的海量终端用户具有高移动性需求,当终端用户移动到新的边缘节点时,边缘节点需要对终端用户重新进行身份认证,即切换重认证。Han等[16]针对无线传感器网络(WSN)中传感器节点的移动性,提出了一种高效的节点认证和密钥交换

协议，使得移动节点重新认证的效率提高了2~3倍，大大减少了节点重新认证的计算开销，并提供移动节点的不可追踪性。Fantacci等[17]提出了一种无需基站BS参与的支持无线传感器网络中移动节点身份认证的协议，该协议基于使用多项式函数来生成分布式双向身份认证的方法，不仅可以允许后续多次认证，且在认证速度方面表现出良好的性能。房帅磊[18]提出了一种基于双因子组合公钥的移动节点认证方案，该方案在移动节点发生切换重认证之前通过引入切换预认证，使得移动节点提前与被切换子网协商出会话密钥，完成资源预约，之后移动节点通过提前协商的会话密钥快速完成切换重认证，该方式极大提高了切换重认证速度，解决了传统认证方案针对移动节点认证效率低，且不适合大规模部署的问题。

3.2 通信安全协议

目前，国际标准化组织IEEE和IETF已为工业物联网制定了一套高可靠、低功耗、可接入互联网的无线通信协议，IEEE工作组主要负责制定链路层以下标准，如IEEE802.15.4-2006标准[19]，其中IEEE802.15.4e[20]是最新版的链路层的标准。IETF工作组主要负责制定链路层以上标准，包括适配层6LoWPAN[21]网络层IPv6RPL[22]与应用层CoAP[23]标准。然而，这些通信协议仍然存在着不少严重的安全问题，文献[24-25]指出了这些协议存在的多种安全漏洞。近年来，随着物联网技术的深入研究，一些兼顾安全性和高效性的通信协议安全方案被陆续提出，对边缘计算同样具有较高的参考价值。

杨伟等[26]针对基于IEEE802.15.4e标准的工业物联网中时间同步协议安全性不足问题，提出一个安全时间同步策略，首先，提出了Sec_ASN算法保护单跳的ASN时间同步和TOF算法保护单跳的Device-to-Device时间同步；其次，提出了Rank-based入侵检测算法来保护多跳时间同步；最后，通过理论分析和实验证明，该安全时间同步策略具有时间同步精度高和开销低特点，并且能够有效防御外部攻击和内部攻击。Raza等[27]指出现有的IEEE 802.15.4链路层安全不提供所需的端到端安全，因此提出了一种通过6LoWPAN扩展实现的IPsec安全方案，并对二者进行了性能比较。结果表明，随着IP数据包和跳数的增长，IPsec扩展比链路层安全性更好，大大节省了时间和资源。

边缘计算在进行计算和通信时还必须考虑到适合设备能力的协议，文献[28]讨论了CoAP协议是IETF为物联网设计的一个适合资源受限设备的协议，CoAP在UDP上运行以保持整体实现的轻量级，大大减少了通信开销，尽管CoAP是为物联网和M2M(Machine to Machine)通信而创建，但它却不包括任何内置的安全功能。DTLS(Datagram Transport Layer Security)协议被用来保护CoAP协议，它提供身份认证、数据完整性、机密性、自动密钥管理和加密算法等安全性功能。

3.3 入侵检测技术

入侵检测技术通过包括监测、分析、响应和协同等一系列功能，能够发现系统主机侧或网络侧未经授权的网络行为或异常现象。目前，入侵检测技术应用大部分侧重于云计算，随着边缘计算的兴起，业界对边缘计算的入侵检测技术也开始进行各种研究，许多在云计算环境下的研究对边缘计算入侵检测技术同样具有参考价值。部分研究学者对边缘计算的入侵检测技术提出了具有针对性的研究方案。

李忠成等[29]提出了一种适用于边缘计算环境的改进极限学习机的入侵检测算法TSS-ELM，该算法增加了云服务器训练样本筛选环节来优化机器学习中的外权，在准确性、时间依赖性、鲁棒性和误报率等方面性能表现优异。Sanjay[30]提出了一种分布式入侵检测系统(DIDS)，入侵检测系统模型被部署在每个云计算区域，当其中一个云计算区域遭受到攻击时，入侵检测系统就会向其他区域发送警报，并评估这些警报的可靠性，如果警报被视为一种新的攻击，则将新的阻止规则添加到阻止列表中，该系统有效提高了检测准确率和检测速度，不断增强了系统自身的安全性。Hosseinpour等[31]提出了一种基于人工免疫系统(AIS)的新型分布式轻量级入侵检测系统，该系统分布在3层物联网结构中，包括云层、雾层和边缘层，在云层，对主要网络流量进行聚类并训练其检测器；在雾层，利用智能数据概念分析入侵警报；在边缘层，将检测器部署在边缘设备中，可以实现轻量级和高效的入侵检测，为检测无声攻击提供了途径。

3.4 隐私保护技术

分布式边缘节点的计算能力虽然大大缓解了数据中心的负载压力，但由于边缘节点靠近用户终

端设备,可以直接收集用户隐私数据,且计算和存储资源受限,网络异构、复杂及服务多样,极易造成用户隐私数据信息的被动泄露的潜在风险。本部分内容将从全同态加密、差分隐私保护、安全多方计算3个方面对各计算模式中的隐私保护技术进行介绍和分析。

3.4.1 全同态加密

全同态加密(Fully Homomorphic Encryption,FHE)是一种允许直接对密文进行操作的加密算法,可以满足边缘计算中数据分布式计算和存储、密文检索以及委托不信任的第三方对数据进行处理等需求,能在很大程度上解决边缘计算中用户的隐私泄露问题。

Gentry等[32]提出了一种基于近似特征向量技术的全同态加密方案,并以此构建了第一个基于身份的全同态加密方案以及基于属性的电路加密方案。针对边缘计算环境下用户复杂多样的特性,刘青等[33]提出了一种基于策略的多用户全同态加密方案,该方案通过在密文中设定适当的访问策略以及在密钥中设定属性,达到对多用户密文的全同态运算以及多用户共享的目的,可以抵制共谋攻击,高效实现密文数据的全同态运算,并支持细粒度的访问控制。

3.4.2 差分隐私保护

差分隐私保护是一种基于数据失真的隐私保护技术,可以在攻击者掌握任意背景知识的情况下对发布数据提供隐私保护,其过程就是通过对真实敏感数据添加噪声使其失真,并保证数据在被干扰后某些数据属性(如统计特性等)能保持不变。目前,面向边缘计算的差分隐私保护技术还处于探索阶段,相关研究者提出了多种环境下的差分隐私保护方案。

陈前[34]将标准的差分隐私理论扩展到分布式的边缘计算环境中,提出了一种基于差分隐私的轻量级室内定位隐私保护方法EC-DPELM,该方法基于边缘计算架构,在网络的边缘侧分布式训练定位模型,将完整的Wi-Fi指纹定位数据拆分并通过隐私保护处理后,发送至边缘节点及边缘服务器进行深度隐私保护和结果聚合,经实验证明,可以有效保证室内定位的隐私性和准确性,没有增加额外的资源开销,为相关边缘计算位置隐私问题和需求提供了切实可行的参考。Wang等[35]提出了一种在移动边缘计算中基于噪声添加的用户位置指纹隐私保护方案LoPEC,该方案提供了一种基于原始噪声生成的优化算法,在连续定位时可以进一步生成轨迹状噪声指纹更新,同时考虑了单点定位隐私和轨迹隐私,可以迷惑潜在的攻击者并防止其在移动边缘计算场景中识别用户的位置。该方案无需任何附加系统,可以直接在智能设备和移动互联网生态系统中实现,大大降低了计算成本。Dwork等[36-37]在满足差分隐私的前提下提出了用户级别的泛隐私概念,基于流算法的思想,可以抵御连续不间断的入侵。

3.4.3 安全多方计算

随着云计算、边缘计算等计算模式的深入发展,计算任务的参考方不断增多,面临的外部环境也越来越复杂多变,需要使用基于基础密码算法的安全协议。安全多方计算(Secure Mutiparty Computation,SMC)作为一种分布式环境下的隐私保护计算方法,最早源自姚期智院士于1982年提出的百万富翁问题[38],其主要思想是在互不信任的多用户网络中,两个或多个参与方协同完成某个功能函数的合作计算,要求每个参与方只能知道这个函数的输出结果,而不能泄露参与方输入的任何隐私信息,即在保证各自隐私安全的前提下通过合作计算获得想要的结果。安全多方计算的这一特点,对于边缘计算环境下的隐私保护有着独特的优势。

Asharov等[39]提出了一种基于安全多方计算的信誉系统模型。与安全多方计算的标准模型不同,该模型中所有参与方都获得了有关其他参与方的诚实度以及信任级别信息,因此可以实现比标准模型更多的功能。该信誉系统模型如果被应用到边缘计算服务中,将对边缘计算用户隐私保护起到很好的促进作用。刘浩东[40]提出了一种基于安全多方计算的"安全隔离森林"的异常检测算法,多个数据拥有者在自身数据集上训练出异常检测模型,加密后广播该模型,其他方接收到加密过的检测模型后,结合单一计算外包服务器,计算得出异常检测结果。该方案通过借助外包计算技术,使得数据拥有者只需做少量的计算且无需将数据加密上传,大大降低了用户端的计算和通信开销,对边缘计算的隐私保护具有借鉴作用。

4 结论

本文首先介绍了边缘计算的基本概念,然后从边缘计算的安全需求出发,围绕身份认证、通信安

全协议、入侵检测以及隐私保护等关键技术，系统阐述和分析了边缘计算安全与隐私保护领域的国内外研究成果。由于边缘计算自身所具有的特性，使得其安全与隐私保护方面仍然面临着诸多挑战，未来边缘计算的安全与隐私保护的研究方向包括以下方面：

(1)在边缘计算环境下，传统的安全防护技术在网络边缘侧存在很大局限，难以有效部署，被动的安全防御很难起到良好效果，因此需要采取更加积极主动的安全防御措施。例如，可以考虑在边缘计算中心内，通过对设备产生的各类日志信息进行分析，来对网络的安全状况进行风险评估，甚至可以在边缘计算中心之间进行联动协作，建立基于边缘计算大数据的分布式的态势感知平台，提高系统的监控和响应能力，最大限度地保证边缘计算系统的安全性。

(2)边缘计算的安全防护技术大多需要在分散的、更靠近用户侧的边缘节点上进行部署，由于边缘节点的计算和存储资源能力有限，无法承载传统网络安全防护技术所需要的大的系统开销。因此，如何实现轻量级的边缘计算安全与隐私保护新方法仍是值得深入研究的重要方向。

(3)目前，针对边缘计算的各种安全与隐私保护策略是基于具体的应用场景而给出的，是具有特殊针对性的一些安全解决方案，但这些方案之间并没有形成一定的通用性。因此，针对边缘计算不同应用场景中所存在的安全问题需要有统一的定义，并形成标准化和通用性的解决方案，这也是下一步工作需要研究的重点。

参考文献

[1] FOX A, GRIFFITH R, JOSEPH A, et al. Above the clouds: a Berkeley view of cloud computing[R]. Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, 2009, 28(13).

[2] Xiao Renyi. Survey of privacy preserving data queries in cloud computing[J]. Journal on Communications, 2014, 35(12): 168-177.

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

[4] YU W, LIANG F, HE X, et al. A survey on the edge computing for the Internet of Things[J]. IEEE Access, 2017(6): 6900-6919.

[5] 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.

[6] 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.

[7] BS PD ISO/IEC TR 23188-2020, Information technology-Cloud computing-Edge computing landscape[S]. 2020-02.

[8] 边缘计算产业联盟，工业互联网产业联盟. 边缘计算参考架构 3.0[Z]. 2018.

[9] 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.

[10] 孙长华，刘斌. 分布式拒绝服务攻击研究新进展综述[J]. 电子学报，2009，37(7)：1562-1570.

[11] 杨伟，何杰，万亚东，等. 物联网通信协议的安全研究综述[J]. 计算机科学，2018，45(12)：32-41.

[12] 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: 71-83.

[13] ECHEVERRÍA S, KLINEDINST D, WILLIAMS K, et al. Establishing trusted identities in disconnected edge environments[C]//2016 IEEE/ACM Symposium on Edge Computing(SEC). IEEE, 2016: 51-63.

[14] 朱智强. 混合云服务安全若干理论与关键技术研究[D]. 武汉：武汉大学，2011.

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

[16] HAN K, KIM K, SHON T. Untraceable mobile node authentication in WSN[J]. Sensors, 2010, 10(5): 4410-4429.

[17] FANTACCI R, CHITI F, MACCARI L. Fast distributed bi-directional authentication for wireless sensor networks[J]. Security & Communication Networks, 2010, 1(1): 17-24.

[18] 房帅磊. 层次化无线传感器网络移动节点认证技术研究[D]. 西安：西安电子科技大学，2011.

[19] ROBERT F, JAMES D, PATRICK W, et al. IEEE standard for local and metropolitan area networks-part 15.4: low-rate wireless personal area networks LR-WPANs)[S]. NewYork: LAN/MAN Standards Committee, 2006.

[20] ROBERT F, RICK A, PATRICK W, et al. 802.15.4e-2012: IEEE standard for local and metropolitan area networks-part 15.4: low-rate wireless personal area networks (LR-WPANs) amendment 1[S]. New York: LAN/MAN Standards Committee, 2012.

[21] KUSHALNAGAR N, MONTENEGRO G, SCHUMACHER C. IPv6 over low-power wireless personal area networks 6LoW-PANs): overview, assumptions, problem statement, and goals, RFC 4919[R]. New York: Internet Engineering Task Force, 2007.

[22] THUBERT P, WINTER T, BRANDT A, et al. RPL: IPv6 routing protocol for low power and lossy networks[R]. New York: Internet Engineering Task Force, 2012.

[23] BORMANN C, CASTELLANI A P, SHELBY Z. Coap: an application protocol for billions of tiny Internet nodes[J]. IEEE Internet Computing, 2012, 16(2): 62-67.

[24] SAJJAD S M, YOUSAF M. Security analysis of IEEE 802.15.4MAC in the context of Internet of Things (IoT)[C]//Information Assurance and Cyber Security. IEEE, 2014: 9-14.

[25] YANG W, WANG Q, QI Y, et al. Time synchronization attacksin IEEE802.15.4e networks[C]//International Conference on Identification, Information and Knowledge in the Internet of Things. IEEE, 2014: 166-169.

[26] 杨伟, 何杰, 万亚东, 等. 基于IEEE802.15.4e标准的工业物联网安全时间同步策略[J]. 计算机研究与发展, 2017, 54(9): 2032-2043.

[27] RAZA S, DUQUENNOY S, HÖGLUND J, et al. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN[J]. Security and Communication Networks, 2014, 7(12): 2654-2668.

[28] AL-FUQAHA A, GUIZANI M, MOHAMMADI M, et al. Internet of Things: a survey on enabling technologies, protocols, and applications[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2347-2376.

[29] 李忠成, 高惠燕, 张文祥. 边缘计算中改进ELM的高效入侵检测算法[J/OL]. 计算机测量与控制: 1-8. [2021-06-22]. http://kns.cnki.net/kcms/detail/11.4762.TP.20210419.1537.022.html.

[30] SANJAY RAM M. Secure cloud computing based on mutual intrusion detection system[J]. International Journal of Computer Application, 2012, 1(2): 57-67.

[31] HOSSEINPOUR F, VAHDANI AMOLI P, PLOSILA J, et al. An intrusion detection system for fog computing and IoT based logistic systems using a smart data approach[J]. International Journal of Digital Content Technology and Its Applications, 2016, 10(5): 34-46.

[32] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based[C]//Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2013: 75-92.

[33] 刘青, 李陶深, 黄汝维. 云计算环境中基于策略的多用户全同态加密方法[J]. 广西大学学报(自然科学版), 2016, 41(3): 786-795.

[34] 陈前. 边缘计算差分私有位置隐私保护研究[D]. 兰州: 兰州交通大学, 2020.

[35] WANG Y, TIAN Z, SU S, et al. Preserving location privacy in mobile edge computing[C]//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.

[36] DWORK C, NAOR M, PITASSI T, et al. Pan-private streaming algorithms[C]//ICS, 2010: 66-80.

[37] DWORK C, NAOR M, PITASSI T, et al. Differential privacy under continual observation[C]//Proceedings of the Forty-second ACM Symposium on Theory of Computing, 2010: 715-724.

[38] YAO A C. Protocols for secure computations[C]//23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). IEEE, 1982: 160-164.

[39] ASHAROV G, LINDELL Y, ZAROSIM H. Fair and efficient secure multiparty computation with reputation systems[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2013: 201-220.

[40] 刘浩东. 基于安全多方计算的隐私保护异常检测算法的外包计算[D]. 哈尔滨: 哈尔滨工业大学, 2017.

(收稿日期: 2022-05-21)

作者简介:

沈传年(1981-), 男, 硕士, 工程师, 主要研究方向: 无线通信、数据安全、区块链等。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部