

移动边缘计算环境下的数据安全与隐私保护 技术综述

杨颖, 任爽

(北京交通大学 计算机科学与技术学院, 北京 100044)

摘要: 移动边缘计算作为云计算的延伸拓展, 其核心目标为将计算、存储及网络功能部署于更贴近最终用户的网络边缘位置。凭借在显著降低延迟、有效提升带宽利用率等方面的突出优势, 移动边缘计算备受行业关注。然而, 其分布式架构特性以及严格的实时性要求也使得它在安全防护与隐私保护方面面临着一系列严峻挑战。全面审视移动边缘计算环境下的安全与隐私问题, 并强调跨学科合作的重要性。首先, 解释移动边缘计算的概念和特点, 并比较其与传统云计算的不同之处以及对现代应用的影响; 其次, 探讨移动边缘计算架构的演进及其与安全措施的关系, 梳理近年来的主要应用场景; 再次, 进一步深入分析移动边缘计算中数据安全和隐私保护的目标、面临的威胁及关键应对策略; 最后, 综合讨论未来可能面临的问题和研究方向。安全和隐私对于移动边缘计算的成功部署具有关键作用, 需要持续研究和跨学科合作来应对不断变化的挑战, 以确保数据与隐私的完整性和机密性。

关键词: 移动边缘计算; 分布式架构; 数据安全; 隐私保护

DOI: 10.11907/rjdk.242062

中图分类号: TP183

文献标识码: A

文章编号: 1672-7800(2026)003-0130-11

扫描二维码阅读全文: 

A Survey on Data Security and Privacy Protection Technology in Mobile Edge Computing Environment

YANG Ying, REN Shuang

(School of Computer Science and Technology, Beijing Jiaotong University, Beijing 100044, China)

Abstract: As an extension of cloud computing, mobile edge computing's core goal is to deploy computing, storage and network functions at the edge of the network closer to the end user. With its outstanding advantages in significantly reducing latency and effectively improving bandwidth utilization, mobile edge computing has attracted industry attention. However, its distributed architecture characteristics and strict real-time requirements also pose a series of severe challenges in terms of security and privacy protection. A comprehensive review of security and privacy issues in the mobile edge computing environment, and emphasis on the importance of interdisciplinary cooperation. First, the concept and characteristics of mobile edge computing are explained, and its differences from traditional cloud computing and its impact on modern applications are compared; Secondly, discuss the evolution of mobile edge computing architecture and its relationship with security measures, and sort out the main application scenarios in recent years; Thirdly, further in-depth analysis of data security and privacy protection goals, threats and key coping strategies in mobile edge computing; Finally, a comprehensive discussion will be held on potential future issues and research directions. Security and privacy play a key role in the successful deployment of mobile edge computing. Continuous research and interdisciplinary cooperation are needed to meet the changing challenges to ensure the integrity and confidentiality of data and privacy.

Key Words: mobile edge computing; distributed architecture; data security; privacy protection

收稿日期: 2024-12-25

基金项目: 国家自然科学基金项目 (62072025)

作者简介: 杨颖 (2000-), 女, 北京交通大学计算机科学与技术学院硕士研究生, 研究方向为边缘计算、虚拟现实技术; 任爽 (1981-), 男, 博士, 北京交通大学计算机科学与技术学院副教授、博士生导师, 研究方向为机器学习、计算机视觉、虚拟现实技术。本文通讯作者: 任爽。

0 引言

移动边缘计算(Mobile Edge Computing, MEC)作为一种新兴的计算模式,因其在降低延迟、提升带宽利用率和增强位置感知等方面的显著优势而受到广泛关注。MEC通过将计算和数据处理能力推向网络边缘,满足了5G和物联网等应用对快速响应和高效数据处理的需求。然而,这种架构的分布式特性和对实时性的追求也引起一系列数据安全与隐私保护的挑战。在MEC环境中,数据的产生、处理和存储多在网络边缘进行,边缘节点由于物理安全措施较弱,更容易受到攻击。同时,MEC网络中设备的异构性和资源限制也使得实施统一的安全策略变得复杂。鉴于MEC在智能交通、智慧城市、工业物联网等领域的广泛应用,其数据安全与隐私保护技术研究具有重要的理论意义和实践价值。一方面,加强MEC环境下的数据安全可以防止敏感信息泄露,保护用户隐私,增强系统的可靠性和信任度;另一方面,有效的隐私保护技术能够确保用户数据的合规使用,避免因隐私泄露而引发的法律和伦理问题。

目前国内外关于MEC的综述很多,但大多是对实际应用的详细描述,在安全和隐私方面还不够完善。为此,本文在前人工作的基础上进行归纳与完善,首先概述了MEC的定义与特性,并讨论了其与传统云计算的区别及其对现代应用的影响;其次,分析了MEC架构及其发展,以及在不同领域的主要应用;再次,详细讨论了MEC中数据安全的定义与目标、面临的安全挑战、典型的攻击与防御机制,以及MEC中隐私保护的基本概念与目标、隐私风险及现有的隐私保护技术;最后,综合分析了数据安全与隐私保护技术在MEC中的融合应用,并对未来的挑战与研究方向进行了展望。

1 MEC概述

1.1 MEC的定义与特性

MEC由欧洲电信标准协会(European Telecommunications Standards Institute, ETSI)于2014年提出,代表了一种计算模式的转变。其将计算和数据处理能力推向网络边缘,即靠近数据源的位置,例如移动基站或路由器。这种架构有助于减少数据传输的时延,并提升带宽的使用效率^[1]。传统云计算通常将数据发送到远程数据中心进行处理,需要将大量数据传输到云端;而MEC将计算和存储资源部署在网络边缘,实现了数据的本地处理,减轻了对中心网络的依赖^[2]。例如,基站和Wi-Fi接入点作为边缘节点,不仅负责数据传输,而且能直接处理数据和执行计算任务。边缘节点的分布式特性还允许不同节点协同工作,提升计算效率和系统的可靠性。

MEC的特性包括低延迟、高带宽利用率、位置感知、分布式计算与存储。具体来说,低延迟特性使得数据能够在本地处理,降低数据泄露风险,这对于需要实时响应的应用至关重要^[3];高带宽利用率减轻了核心网络的负载,这对于视频监控和内容分发等带宽密集型应用特别有利;位置感知能力使MEC能够根据用户设备的位置提供本地化服务,例如实时导航和位置相关的广告;分布式计算和存储特性不仅提高了资源利用率,而且增强了系统的可靠性,确保即使部分节点发生故障,系统也能稳定运行。

1.2 MEC的架构与发展

最初,MEC主要应用于移动网络领域,但随着相关技术的发展,ETSI于2017年将MEC的定义扩展为“多接入边缘计算”,使其能够适应Wi-Fi、固定网络和卫星等多种接入技术^[4]。这一变化使得MEC的应用更加灵活,确保了不同设备、网络与平台之间的开放性和互操作性,能够服务于更广泛的网络架构和应用场景。

如图1所示,MEC架构通常由用户设备层、边缘节点层和核心云层组成。用户设备层包括智能手机、物联网设备、自动驾驶车辆等终端设备,用户通过终端设备能够直接访问MEC平台提供的服务,生成大量数据并发送给边缘节点进行处理。边缘计算节点包括移动基站或Wi-Fi接入点等,部署在用户设备附近。边缘节点层为MEC架构的核心,负责数据的本地处理与分析,这些节点的地理位置优势使它们能够提供必要的计算、存储和网络带宽资源,满足应用对低延迟和高带宽的需求。核心云层包含一些边缘服务器及数据中心等,与边缘计算节点紧密协作,用于处理更复杂的、非实时的数据任务,并负责数据的存储与全局整合。ETSI的标准化平台通过提供开放API,使得应用能够高效地访问底层硬件资源,并通过资源管理、任务调度和服务质量保障等功能来优化系统性能。在MEC中,数据在多个节点之间传输与处理,需要在不同环节中均实施有效措施来维护系统安全,如进行数据加密、身份验证、实施安全传输协议等。

1.3 MEC的主要应用领域

MEC技术已经在多个领域展现出应用潜力,特别是在需要低延迟、高带宽、位置感知和实时数据处理的场景中。例如,在环境监测领域,期治博等^[5]提出基于机器学习算法的边缘端视频协同分析方法,通过减少多摄像头实时视频数据的处理量来有效提升系统的准确率和效率。栾凌等^[6]构建了基于边缘计算的输变电工程全环节单元确认的精准造价智能管控模型,利用MEC高可靠性的优势实现了高精度的全环节各单元造价管控。在智能交通领域,MEC与车联网技术的结合推动了自动驾驶和交通管理的进步。通过在路侧基础设施,如基站或交通灯中部署边缘节点,MEC能够实现车辆间的实时信息交换,车辆也能够及时获取交通数据和周围环境信息,从而作出快速反应,保障行车安全^[7]。例如,El-Sayed等^[8]将MEC集成到智能

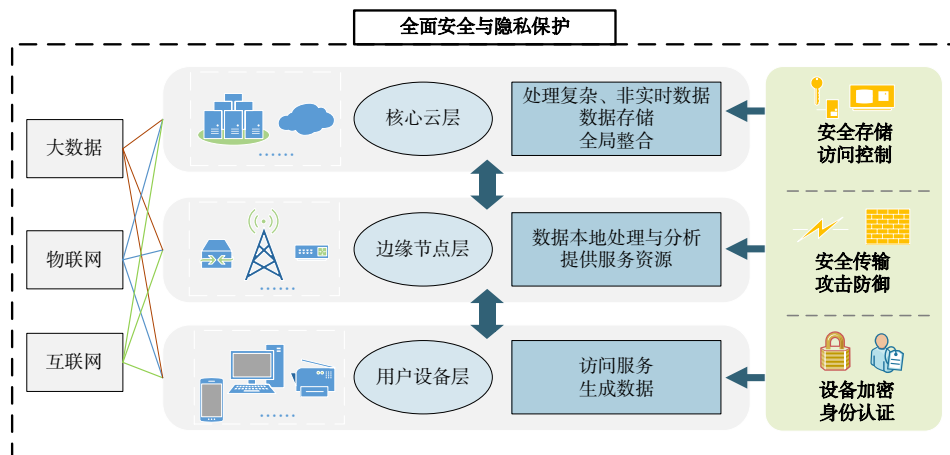


Fig. 1 MEC architecture considering security and privacy protection

图1 考虑安全与隐私保护的MEC架构

交通系统中,用于监控车辆位置和状态,对异常情况作出快速响应。Wang等^[9]提出基于MEC的网约车优化调度方法,响应更快且调度策略更合理。韦睿等^[10]基于MEC和软件定义网络,提出一种从宏基站到MEC服务器,再到车联网架构的任务卸载方案,相较于其他常用方法能够得到更高的系统效用。在工业物联网方面,MEC被用于智能制造和生产自动化。例如,Bellavista等^[11]利用MEC实现数据的本地处理,监控生产线设备状态,及时发现并响应异常情况。Zhang等^[12]提出一种集成数字孪生与多接入边缘计算的新型框架,用于构建支持安全知识共享、具备超低延迟性能的智能机床群。虚拟现实(Virtual Reality, VR)和增强现实(Augmented Reality, AR)领域对数据传输速率的要求较高,且对传输时延的敏感性强,MEC可通过减少计算延迟为其提供更流畅的用户体验。例如,谭彬等^[13]设计了完整的移动边缘云VR系统,包括基于视点的VR处理和混合数模传输优化,实现了更加稳健高效的传输。Zhou等^[14]设计了一种新颖的车辆到边缘基础设施,将计算单元与基站和聚合点共存,实现了计算资源的边缘部署,确保AR应用在带宽受限或高延迟环境下仍能稳定运行。Chuang等^[15]将MEC应用于VR游戏中,使得多人互动更加同步,增强了游戏的沉浸感。随着MEC技术的快速发展,其强大的实时数据处理和本地化计算能力将发挥更大作用,成为推动各行业数字化转型的关键技术。

2 MEC的数据安全与隐私保护问题

2.1 数据安全与隐私保护的定义与目标

最初,网络安全被定义为保护通信网络免受可能的入侵和漏洞攻击的手段。这些攻击和威胁仅限于中间人、中继和欺骗等干预和伪装攻击,通过足够级别的加密和加密原语可以一定程度上缓解可能的攻击。然而,新型的通信服务优先考虑网络的数据速率以服务更多用户,因此繁琐的加密原语是不明智的。此外,如Afolabi等^[16]所述,软件定义网络、网络功能虚拟化和网络切片的软件化方法对

安全保障提出了更多要求。大多数新兴系统,包括MEC系统,都是数据信息物理系统(Cyber-Physical Systems, CPS),它们集成了计算、网络和物理过程,以创建扩展到网络和物理空间的环境。国际标准化组织和国际电工委员会联合发布了ISO/IEC 27002标准,为信息安全管理体系提供了详尽的控制措施和实施指南。该标准将数据信息安全定义为对数据保密性、完整性和可用性的保护,这三项原则构成了信息安全的基础,通常被称为CIA(Confidentiality-Integrity-Availability)三元组^[17]。具体如图2所示。其中,保密性的目标为确保数据只能被授权用户或设备访问,防止敏感信息泄露;完整性要求数据在传输和存储过程中不被非法篡改,并且能够及时发现和阻止未授权的修改;可用性用于保证授权用户需要时能够访问数据和服务。Schatz等^[18]提出一个新的网络安全定义,即国家和组织为保护网络空间数据和资产的CIA而遵循的安全管理流程相关方法和行动,网络安全的最新要求已超出CIA,可追溯性、身份验证、授权、匿名化、粒度、本地化和信任等因素是网络安全适用系统的新要求。

隐私是指个人对其行为、信息及空间享有自主控制权,并有权在未经其明确、自愿同意的情况下,免受任何形

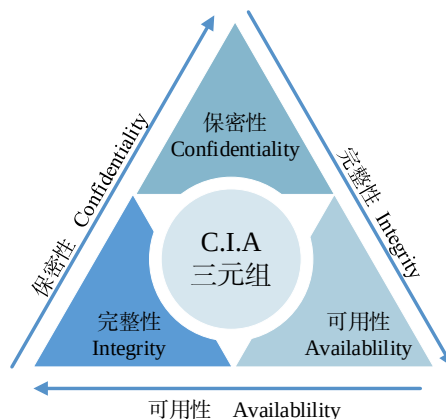


Fig. 2 Three principles of information security

图2 信息安全的三项原则

式的记录、监视或数据收集活动的干涉。在数字环境中,服务提供商不得在未经用户同意的情况下滥用其数据,应采取措施保护用户身份,同时使用户行为不可追踪。拥有用户个人数据的不负责任的实体可能会选择将其外包给外部机构,以推导出个人意图、行为或利益,从而扩大其商业市场。此外,攻击者可通过保护薄弱的系统用户凭证去侵犯用户的个人隐私,窃取个人信息,这些非法行为需要通过立法、加强隐私保护措施等进行限制。在 MEC 领域,隐私保护的目标为确保 MEC 环境中的隐私安全和合规,具体包括全球范围内的隐私政策立法,需考虑各方利益;MEC 服务提供商对隐私违规负责,消费者需报告违规;整合技术时建立共同隐私行为准则^[19];保障数据在 MEC 服务提供商间可迁移;明确各方数据处理责任,保持透明度^[20];公布用户实体的最小规格要求以确保隐私性;优化用户实体资源利用,嵌入隐私保护机制^[21]。

数据安全为隐私保护提供了技术保障,实现隐私保护也印证了数据安全的 3 项基本原则。数据安全侧重于确保数据不被非法访问、篡改或丢失,其核心为数据保护;而隐私保护侧重于保障个人对其数据的控制权,防止数据被滥用或泄露,确保个体隐私不受侵犯。两者的共同目标为确保信息的安全性和个人的隐私权,在 MEC 环境中,二者相互依存,互为支撑。

2.2 MEC 面临的安全挑战与隐私风险

在数据安全方面,MEC 将计算和数据处理任务迁移到网络边缘,即边缘节点,这些节点通常位于物理安全性较低的开放环境中,因此更容易受到各种安全威胁。如表 1 所示,MEC 面临的安全挑战可以从以下几个方面展开探讨:

首先,是边缘节点的脆弱性问题。由于这些节点通常位于较为开放的环境中,物理安全措施较弱,与数据中心相比,更容易受到分布式拒绝服务攻击、侧信道攻击、恶意软件注入攻击、身份验证和授权攻击、欺骗攻击等^[22-23]。攻击者可能会利用恶意流量淹没边缘节点,导致服务中断,甚至传播恶意代码以控制节点。其次,是设备异构性问题。MEC 网络中设备种类繁多,使用的操作系统、协议和安全机制各不相同,这使得实施统一的安全策略变得困难。系统遭受攻击的难易程度不仅与异构性有关,而且会随着异构程度的增加而增加^[24]。尤其是物联网设备,由于缺乏标准化安全机制,共享的设备授权数据管理方式各异,更容易遭受攻击和泄露数据^[25]。再次,是 MEC 架构集中管理困难的问题。每个边缘节点需要独立部署安全措施,而碍于资源限制,无法为边缘节点提供与中心化数据中心相同级别的保护,降低了攻击检测和保护响应的效率。数据共享不可避免,因此需重点考虑去中心化的访问控制、负载均衡、恶意用户追踪等策略,灵活采用多种防御机制应对攻击^[26]。最后,是资源限制问题。边缘节点的计

算能力、存储空间和电池电量往往有限,限制了复杂加密算法和安全验证机制的高效运行,尤其是在对实时性要求较高的应用场景中。Wang 等^[27]认为需要重点考虑一些资源友好型方法,例如使用更加轻量高效的加密算法或身份认证方法来减少设备间的冗余交互。MEC 需要采用轻量级分布式安全机制来增强边缘节点的安全性,使用兼容多种设备的统一安全框架,并加强隐私保护和合规性管理。

Table 1 Security challenges and solutions faced by MEC

表 1 MEC 面临的安全挑战及其解决方案

安全问题	原因	解决方案
边缘节点脆弱性	节点所处开放环境物理安全措施较弱	采用多种攻击防御机制
	MEC 网络设备各类机制均有差异	
设备异构性	MEC 架构的分布性	
难以集中管理	边缘节点有限的资源难以运行复杂安全措施	使用轻量高效的加密技术
资源限制		

MEC 面临的隐私风险与其架构特点紧密相关。具体如下如表 2 所示。首先,是身份信息泄露问题。边缘节点在处理用户身份标识符和设备信息时,攻击者可能会通过流量监控或节点入侵来窃取这些信息,进而进行身份冒用和欺诈等恶意活动。其次,是位置隐私泄露问题。基于位置的服务为 MEC 用户提供了各种应用服务,许多应用依赖于用户的实时位置数据运行,使得用户的活动轨迹容易被恶意获取与分析。Gilsenan 等^[28]认为用户位置等各种个人信息可能会以弹出式服务请求的方式合法地向第三方透露,订阅者通常会同意,不考虑或未意识到可能带来的后果。攻击者通过分析这些位置数据,可以推测出用户的出行模式和生活习惯,甚至进行定向攻击,给个人隐私甚至人身安全带来威胁。除了直接信道外,广播无线传输的次要移动信道也可能受到窃听者的监控。Miao 等^[29]认为现有基于布隆过滤器的位置信息加密方案可能未考虑到布隆过滤器中未映射信息的冗余位,导致计算开销较大,且会暴露布隆过滤器中的包含关系。

Table 2 Privacy risks faced by MEC and their solutions

表 2 MEC 面临的隐私风险及其解决方案

隐私风险	原因	解决方案
身份信息泄露	大数据应用会产生大量个人隐私数据	流量监控、攻击检测、访问控制等
位置隐私泄露	许多应用依赖于实时位置数据	攻击检测、物理安全等
关联攻击	MEC 设备使用的数据具有高度关联性	异常检测、数据隔离等

此外,数据推断和关联攻击也加剧了隐私风险。MEC 节点的设备使用数据、传感器数据等信息具有高度关联性,攻击者可通过跨数据源关联分析推测出用户的敏感信息。即使数据经过匿名处理,多个来源的信息交叉分析仍可能泄露用户的部分行为与特征。MEC 节点通常会为多个应用和用户提供服务,如果数据隔离机制不严格,不同

用户或应用的数据也可能无意间被泄露。

总体来看,MEC的分布式架构和本地化数据处理特性使得隐私风险更加突出,尤其是在身份信息泄露、位置数据暴露和多租户的环境下。因此,需要采取更为严密的隐私保护措施,例如提高身份验证、位置数据模糊化和多租户数据隔离等方面的安全性,以便在保护用户隐私的同时充分利用MEC的优势。

3 可用于MEC环境的数据加密与隐私保护技术

3.1 MEC中的典型攻击与防御机制

在MEC环境中,由于网络架构具有分散特性,且边缘节点的计算、能源和通信资源有限,无法进行数据缓存并遵循传统的完全协议,可能会遭遇分布式拒绝服务(Distributed Denial of Service, DDoS)攻击、边信道攻击以及恶意软件注入攻击等,对系统的可用性、数据安全性造成严重威胁。为应对这些威胁,研究者们提出多种防御机制。具体来说,DDoS攻击通过发送大量恶意流量使目标节点资源过载,导致服务中断。在MEC中,由于边缘节点资源有限,DDoS攻击的影响尤为严重。为减轻这种攻击的影响,Tuan等^[30]提出流量过滤技术来识别和过滤异常流量。刘延华等^[31]参考云计算的防御机制,对系统内复杂的流量特征进行分析,提取其相关性并进行实时监测,有效提升了DDoS攻击的检测准确率。Bhushan等^[32]提出一种新颖的流表共享方法来保护基于软件定义网络的云免受流表过载DDoS攻击,具有较高的抵抗力和较低的通信开销。Fu等^[33]提出一种名为Exosphere的检测框架,通过深度语义分析包长度模式来识别隧道中隐藏的泛洪攻击流量,解决了传统方法因加密隧道协议无法检测此类攻击的问题。

边信道攻击利用设备的物理特征,如功耗或电磁辐射来推测设备的敏感信息。Qu等^[34]认为MEC中的设备通常缺乏严格的物理隔离保护,且信道状态信息身份验证有一定的局限性,往往成为边信道攻击的目标。防御边信道攻击的有效手段包括加密和随机化机制。例如,Sasdrich等^[35]通过引入随机性来干扰攻击者的分析,增加攻击难度。Sedjelmaci等^[36]提出一种结合安全专家知识与机器学习能力的混合学习安全框架,用于保护边缘计算网络免受已知和未知攻击,同时最小化误报率。Germain等^[37]利用无线信道的多样性和短期互易性识别合法和非法用户。薛建彬等^[38]在保证每个地面用户最小安全计算要求的前提下,通过联合优化信道系数、发射功率、中央处理单元计算频率、本地计算和无人机轨迹来最大化系统的平均安全计算能力。

恶意软件注入是指攻击者通过植入恶意代码来获取设备控制权,并进一步破坏系统的安全性。在MEC中,由于边缘节点分布广泛且安全防护较弱,它们容易成为恶意软件攻击的目标,还可能受到邪恶孪生体通过网络发起设

备到设备攻击。为提高MEC的防御能力,可以采用定期固件更新、恶意软件行为检测等避免该类攻击。例如,杨志鹏等^[39]利用第三方库隔离机制来防止攻击者构造的恶意模块逃逸出沙箱的限制。董峰等等^[40]提出一种仿照生物免疫系统原理的多层协同检测模型以解决云计算平台中复杂、未知的入侵攻击问题。Moon等^[41]提出一种基于决策树和主机行为分析的入侵检测系统,通过监控异常行为来检测和防御隐蔽且持续的高级持续性威胁攻击。范伟等^[42]构建了一种基于静态贝叶斯博弈的模型,用于解决MEC网络中因资源受限而难以最优响应入侵的问题,从而帮助防御方作出最理性的响应决策。

在MEC环境中,由于资源受限且网络架构分散,防御机制的评估尤为关键。为便于评估不同防御技术的有效性,表3从①计算性能、②通信开销、③延迟与实时性、④安全性、⑤能耗、⑥可扩展性、⑦防御深度几个方面对不同技术进行了全面比较。可以看出,流量过滤技术在MEC环境中表现出色,具有低计算开销、低通信开销和高实时性,适合资源有限的边缘设备。分布式检测与响应机制具备较强的安全性和可扩展性,适用于大规模多节点的部署,但存在较高的通信开销和能耗。加密与随机化机制能有效对抗边信道攻击,但在实时性和能耗方面有所欠缺。未来研究应聚焦于优化防御机制的计算性能和能耗,同时提升其适应性和多层次防御能力,以满足MEC环境的复杂需求。

3.2 适用于MEC环境的数据加密技术

在MEC环境中,由于边缘设备往往资源有限,运行传统的加密算法可能效率不高,轻量级加密技术成为一个实用选择。这些轻量级算法的密钥较短,计算需求较低,更适合资源受限的边缘设备。椭圆曲线加密(Elliptic Curve Cryptography, ECC)是一种流行的轻量级加密技术,其能在使用较短密钥的同时保持较高的安全性,可在无线传感器网络 and 智能设备中保护数据安全。例如,一个256位的ECC密钥可以达到与2 048位RSA(Rivest-Shamir-Adleman)密钥相当的安全级别。Abdaoui等^[43]提出一种基于ECC的新型身份验证与加密方法,该方法使用模糊逻辑生成的随机数而不是移位寄存器,具有更好的性能。高钰洋等^[44]设计了基于GPU的椭圆曲线运算库,通过合理分配存储空间并优化计算量,最大化了运算库的吞吐量与性能。Kishore等^[45]使用ECC建立安全的设备到设备通信协议,为系统提供了极高的安全性,但为了确保系统可用性,用户必须容忍服务延迟。

其他对称加密算法,如PRESENT和Speck,亦适用于资源受限的环境。例如,殷莉等^[46]针对机房软硬件设备计算资源有限的问题,改进了PRESENT算法的框架结构与加密过程,使其具有高吞吐量、低时延、低能耗以及较强的攻击抵御能力。Sleem等^[47]提出基于Speck的新型超轻量级密码算法,具有更好的灵活性和更低的资源需求,并在

Table 3 Comparison of typical defense mechanisms in MEC environment
表 3 MEC 环境中典型的防御机制比较

攻击手段	文献作者	防御机制	性能评价						
			①	②	③	④	⑤	⑥	⑦
DDoS 攻击	Tuan 等 ^[30]	基于机器学习的流量过滤	高	低	高	中	低	高	中
	刘延华等 ^[31]	基于联邦增量学习攻击检测	高	低	高	中	低	高	中
	Bhushan 等 ^[32]	流表共享方法	中	低	中	高	高	高	高
	Fu 等 ^[33]	分析数据包长度模式	中	中	中	高	中	中	高
边信道攻击	Sasdrich 等 ^[35]	引入随机性干扰攻击	中	中	低	高	中	中	高
	Sedjelmaci 等 ^[36]	混合检测攻击者	中	中	低	高	中	中	高
	Germain 等 ^[37]	利用物理特性识别攻击者	高	低	高	高	低	高	高
	薛建彬等 ^[38]	联合优化平均安全计算能力	中	中	低	高	中	中	高
恶意软件注入	杨志鹏等 ^[39]	基于第三方库隔离的 Python 沙箱逃逸防御机制	中	中	中	高	高	中	中
	董峰等 ^[40]	多层免疫入侵检测	中	中	低	高	中	中	高
	Moon 等 ^[41]	基于决策树的行为分析	中	低	中	高	中	中	高
	范伟等 ^[42]	基于静态贝叶斯博弈的入侵响应决策	中	高	中	高	高	高	高

物联网场景中得到了应用。Altaie 等^[48]将 Speck 算法与 PRESENT 算法相结合,可输出更加安全和私密的加密数据。Liu 等^[49]构建了一种新的明文可检验加密方案,可用于在轻量级物联网设备上验证数据拥有者所发送密文的有效性。Dou 等^[50]认为动态可搜索对称加密是云存储领域一种有应用前景的技术,同样可用于对 MEC 环境中的加密数据进行安全搜索。Yang 等^[51]提出一种基于动态共识委员会的安全数据共享方法,使用授权的多接收者可搜索加密,利用区块链动态委员会消除单密钥暴露问题,实现无需配对和动态用户管理的快速关键字搜索。

一些分组加密模式具有高扩散性和错误传播特性,可根据场景需求进行选择。例如,Rana 等^[52]提出改进的 LWBC(Lightweight Block Cipher)分组加密算法,为能耗有限的设备提供有效的加密方案。Guo 等^[53]提出 Shadow 加密方法,在物联网节点中结构紧凑,且具有较高的抗密码分析安全性。Li^[54]将 CTR 加密与 Bloom Filter 数据结构相结合,用于降低大数据的冗余性,适用于需要实时通信的应用,如 AR 和 VR。Roy 等^[55]设计了一种超高速轻量级分组密码算法,可解决资源受限的物联网设备所面临的安全加密需求。轻量级加密技术在多种 MEC 场景中展现出广

泛的应用潜力。在智能家居、车联网和医疗设备等领域,边缘设备通过使用这些轻量级加密技术来保护用户隐私和数据安全,防止信息泄露或被篡改。同时,这些技术还能帮助设备延长使用寿命,提高响应速度,并在资源受限的情况下保持高效的安全性能。

表 4 列举了适用于 MEC 环境的数据加密技术,主要根据①计算性能、②通信开销、③延迟与实时性、④安全性、⑤能耗、⑥可扩展性、⑦兼容性、⑧防御深度 8 个量化指标对其进行综合评估。可以看出,ECC 在计算性能、通信开销和能效方面表现出色,适用于需要高安全性、低计算开销和低延迟的场景,尤其是资源受限的边缘设备中。PRESENT 和 Speck 作为轻量级对称加密算法,具有低能耗、低计算开销和强适应性等优势,适用于大规模物联网设备的加密应用。动态可搜索对称加密算法提供了较强的数据隐私保护能力和动态搜索功能,但需要更多的计算和通信资源,适用于需要高安全性的数据共享和搜索场景。分组加密技术适用于需要高安全性和较强防护能力的场景,但在能效和实时性方面有所折衷。根据应用需求的不同,选择适当的加密技术对于 MEC 环境的安全性和效率至关重要。

Table 4 Comparison of data encryption technologies suitable for MEC environments
表 4 适用于 MEC 环境的数据加密技术比较

加密技术	文献作者	实施方案	性能评价							
			①	②	③	④	⑤	⑥	⑦	⑧
椭圆曲线加密	Abdaoui 等 ^[43]	模糊逻辑生成随机数身份验证	高	低	低	高	高	高	高	中
	高钰洋等 ^[44]	基于 GPU 的椭圆曲线运算库	高	低	低	高	高	高	高	中
	Kishore 等 ^[45]	5G 网络 D2D 安全通信	高	低	高	高	高	高	高	中
PRESENT 加密	殷莉等 ^[46]	针对硬件资源有限的改进算法	高	低	低	中	高	高	高	低
Speck	Sleem 等 ^[47]	物联网超轻量级加密	高	低	低	中	高	高	高	低
	Altaie 等 ^[48]	结合 PRESENT 的混合加密	高	低	低	中	高	高	高	低
明文可验加密	Liu 等 ^[49]	基于区块链的跨域数据共享	中	高	中	高	中	中	中	高
可搜索加密	Dou 等 ^[50]	对云存储加密数据安全搜索	中	高	中	高	中	中	中	高
	Yang 等 ^[51]	基于动态共识委员会的安全数据共享	中	高	中	高	中	中	中	高
	Rana 等 ^[52]	综合平衡安全性与系统效率	中	中	中	高	中	高	中	高
分组加密	Guo 等 ^[53]	物联网中抗密码分析	中	中	中	高	中	高	中	高
	Li ^[54]	结合过滤技术加密与冗余消除	中	中	中	高	中	高	中	高
	Roy 等 ^[55]	资源受限物联网中超快轻量级加密	中	中	中	高	中	高	中	高

3.3 适用于 MEC 环境的隐私保护技术

为了应对 MEC 中的隐私泄露风险,现有隐私保护技术提供了多层次的防护方案,常用的隐私保护技术包括数据匿名化、差分隐私、访问控制、同态加密、零知识证明和安全多方计算等。例如,数据加密通过将个人身份信息从数据中加密、移除或模糊化,避免数据与个体直接关联。数据匿名化将姓名、地址等敏感信息替换为标识符,或使用数据泛化技术降低数据的辨识度,但是其可通过数据关联技术重新被攻击者识别出匿名数据,因此通常与其他隐私保护技术结合使用。例如,Ye 等^[56]在联合学习可逆匿名化框架的基础上引入特定于身份的加密—解密架构。唐小晶等^[57]利用数据隐藏技术修改载体对象,使其包含需要传递的信息,仅有接收者知晓信息传递经过以及信息内容。同态加密是一种在加密数据上直接执行计算的技术,其允许用户在不解密数据的情况下进行运算操作,计算结果在解密后仍保持正确性,广泛应用于需要保护隐私的计算场景。例如,Han 等^[58]将该技术应用于金融交易;Li 等^[59]将该技术应用于车联网数据分析。

差分隐私通过向数据集中加入噪声来确保分析结果不会暴露个体信息,其核心思想为在不改变数据整体统计特性的前提下增加其随机性,从而使攻击者无法从结果中推测出任何个体的具体信息。例如,Liu 等^[60]将差分隐私技术应用于医疗大数据中,用于保护个人健康信息。Cai 等^[61]基于差分隐私的连续数据发布思想提出一种联邦学习框架。Zheng 等^[62]通过向电力数据中注入拉普拉斯噪声来保护敏感用电信息。王琨等^[63]提出基于 Rényi 差分隐私的图卷积协同过滤推荐算法,可在保护数据安全的同时实现隐私性与效用性之间的平衡。Kong 等^[64]提出用于审计差分隐私有效性的测试机制,确保了差分隐私的安全性。

访问控制技术通过限制对敏感数据的访问,确保只有经过授权的用户或设备才能进行操作。在 MEC 环境中,访问控制能有效防止数据滥用和越权访问,这在多租户环境下尤为重要。基于角色的访问控制(Role-based Access Control, RBAC)和基于属性的访问控制(Attribute-Based Access Control, ABAC)是常见的控制策略,其中 RBAC 基于用户角色进行权限管理,而 ABAC 则根据用户属性来设置访问条件。例如,Zhang 等^[65]和周权等^[66]分别使用 RBAC 和 ABAC 结合区块链技术来提高系统的安全性。Wei 等^[67]提出一种针对区块链辅助 6G 多接入边缘计算网络的可信访问控制方法,通过多层级区块链架构和强化学习算法解决异构设备环境下的访问控制挑战。单棣斌等^[68]则考虑实际场景,对大数据动态因素进行分析,提出基于场景感知的访问控制模型。

零知识证明(Zero-Knowledge Proof, ZKP)是一种允许数据持有者在不泄露数据内容的情况下向第三方证明某些信息真实性的技术。在身份验证等场景中,ZKP 能有效

保护用户隐私,避免泄露敏感数据。Ge 等^[69]认为可以使用零信任技术进行身份验证,专注于以代理为中心的信任评估和访问策略,以识别恶意攻击者,并在确保系统性能的同时主动延迟其横向移动。安全多方计算(Secure Multi-Party Computation, SMPC)允许多个参与方在不泄露各自私有数据的情况下共同完成对某个函数的计算,并仅获取或共享计算结果,而无法从计算过程中推断出其他参与方的私有输入信息。Zhao 等^[70]认为该技术特别适用于需要在多个边缘节点之间协同计算并涉及敏感数据的场景,如金融和医疗数据分析。Brüggemann 等^[71]提出一种在已知作弊者存在的情况下可进行快速安全多方计算的方法。Akama 等^[72]提出具有隐私性的安全速率保证协议 Scrappy,允许客户端生成不可伪造、不可链接的速率保证证明,这为服务器提供了客户端没有不当行为的加密保证。Jiang 等^[73]认为位置隐私保护技术通过模糊化位置数据、注入虚假位置或区域分割来保护用户的地理信息不被泄露,在智能交通和位置广告等应用中得到广泛应用。阮华锋等^[74]针对实际场景中 CSP(Cloud Service Providers)之间可能存在的共谋问题,提出基于垂直分割的 MLVP(Machine Learning Vertical Partitioning)方案。Xu 等^[75]通过在硬件层创建隔离的计算环境来保障数据在处理过程中的安全性。

采用①隐私保护强度、②攻击抗性、③计算效率、④存储开销、⑤带宽消耗、⑥可扩展性、⑦技术复杂度、⑧合规性、⑨能源效率 9 个量化指标对以上隐私保护技术其进行综合评估,结果见表 5。可以看出,ECC 和 PRESENT 在 MEC 环境的隐私保护中表现出色,具有较高的计算性能、较低的能耗和通信开销,适用于资源受限的边缘设备。差分隐私提供了强大的隐私保护功能,但在实时性和计算开销上存在一定妥协。同态加密和 ZKP 虽然在隐私保护性能和安全性方面表现优异,但计算开销和能耗较高,影响了其在 MEC 中的广泛应用。访问控制技术则提供了高效的权限管理和数据保护功能,适合与其他隐私保护技术联合使用。未来研究应关注如何平衡隐私保护效果与系统性能,特别是在低功耗、低延迟的环境中。

4 未来挑战与研究方向

随着人工智能技术的发展,边缘设备需要处理越来越多的敏感信息,增加了隐私泄露、数据伪造和对抗样本攻击的风险^[76]。此外,资源限制、边缘设备分散和多租户环境中的数据隔离问题使得安全机制的实施变得更加复杂,整合统一且有效的安全机制仍待研究。机器学习在安全领域有着愈发广泛的应用,但很容易出现微妙的陷阱,从而削弱其性能,并导致基于学习的系统不适合安全任务和实际部署^[77]。由于量子计算的崛起,针对传统加密方法的攻击已成为迫在眉睫的安全威胁,主要是因为量子计算的

Table 5 Comparison of privacy protection techniques for MEC environments
表 5 适用于 MEC 环境的隐私保护技术比较

隐私保护技术	文献作者	保护机制	性能评价								
			①	②	③	④	⑤	⑥	⑦	⑧	⑨
数据加密	Ye 等 ^[56]	联合学习可逆匿名化框架	高	中	高	低	低	高	低	中	高
	唐小品等 ^[57]	信息隐藏算法	高	高	低	中	高	低	高	高	低
	Han 等 ^[58]	同态加密	高	高	低	高	高	低	高	高	低
	Li 等 ^[59]	区块链结合同态加密	高	高	低	高	高	低	高	高	低
差分隐私	Liu 等 ^[60]	机器学习结合差分隐私	高	高	中	中	高	高	中	高	中
	Cai 等 ^[61]	联邦学习结合差分隐私	高	高	中	中	中	高	中	高	中
	Zheng 等 ^[62]	分布式噪声注入	高	高	中	中	中	高	中	高	中
	王琨 ^[63]	基于 Rényi 差分隐私与协同过滤	高	高	高	中	中	高	中	高	中
访问控制	Zhang 等 ^[65]	结合区块链去中心化访问控制	高	中	高	低	低	高	低	高	高
	周权等 ^[66]	结合区块链的国密轻量级访问控制	高	中	高	低	低	高	低	高	高
	Wei 等 ^[67]	结合区块链的多路访问控制	高	中	高	低	低	高	低	高	中
	单棣斌等 ^[68]	基于场景感知的动态访问控制	高	中	高	低	低	高	低	高	高
其他方法	Ge 等 ^[69]	博弈论零信任身份验证	高	高	中	中	高	中	低	高	中
	Zhao 等 ^[70]	安全多方计算	高	高	低	中	高	中	高	高	低
	Brüggemann 等 ^[71]	已知恶意第三方场景下的快速安全多方计算	高	高	低	中	高	中	高	高	低
	Akama 等 ^[72]	保护安全的速率限制系统	高	中	高	低	低	高	高	高	高
	Jiang 等 ^[73]	模糊化与注入虚假数据	中	中	高	低	低	高	低	中	高
	阮华锋等 ^[74]	垂直分割与机器学习	高	高	中	中	高	中	高	高	低
	Xu 等 ^[75]	可信执行环境	高	高	高	低	低	中	高	高	高

强大计算能力能够破解基于数学复杂性的传统加密技术^[68, 78]。在当今基于云的量子计算机环境中,用户缺乏对计算机的物理控制,因此物理攻击可用于提取在计算机上执行的敏感信息,如何防御针对量子计算系统的旁道攻击是需要考虑的新问题^[79]。

面对以上挑战,未来研究可能集中在以下几个领域:①利用 AI 技术提升 MEC 的安全性,通过机器学习和深度学习算法分析数据流,研究更实用的安全模型^[80];②探索如何在保护隐私的同时保证群组内数据共享的安全性以及以群组方式高效地共享外包数据,可采用密钥协商、差分隐私、安全多方计算等技术^[81];③区块链技术的应用可为服务提供商和数据所有者提供处理个人数据的去中心化机制,也可利用其高级功能来增强数据来源的透明度^[82];④开发适合边缘设备的轻量级加密技术和抗量子计算加密技术,如探讨利用算法检测量子算法中是否有违规行为^[83];⑤在硬件安全方面,物理不可克隆函数和可信执行环境可以为边缘设备提供更强的安全保护,可针对 MEC 的分布式特性研究分布式安全机制、防御手段等^[84-85];⑥在多租户环境中,沙箱技术和虚拟化技术可以为每个租户提供隔离的运行环境,防止数据泄露;⑦基于隐私保护的动态风险评估模型有助于实时监控和调整安全策略,以应对不断变化的安全威胁。

5 结语

MEC 因具有低延迟、高带宽利用率和强位置感知等优势而受到广泛关注,但其分布式特性和对实时性的追求也带来了数据安全和隐私保护的挑战。本文综合分析了

MEC 环境中的数据安全和隐私保护技术,首先介绍了 MEC 的定义和特点,并与传统云计算进行了比较;其次分析了 MEC 的发展与主要应用;再次探讨了 MEC 中数据安全和隐私保护的基本目标、面临的风险和常见对策;最后对该领域未来的挑战和研究方向进行了讨论。MEC 在多个领域具有巨大的应用潜力,而随着科学技术的进步,各行各业对安全和隐私保护的需求持续增加。未来研究需要在保证 MEC 效率的同时加强数据安全和隐私保护,以应对不断变化的安全威胁,这需要技术创新,以及政策、法规和伦理的共同进步。

参考文献:

[1] SPINELLI F, MANCUSO V. Toward enabled industrial verticals in 5G: a survey on MEC-based approaches to provisioning and flexibility[J]. IEEE Communications Surveys & Tutorials, 2020, 23(1): 596-630.

[2] ZHAO M. Survey on technology and application of edge computing[J]. Computer Science, 2020, 47(S1): 268-272, 282.
赵明. 边缘计算技术及应用综述[J]. 计算机科学, 2020, 47(S1): 268-272, 282.

[3] SUN J M, ZHAO M X. Survey of application of differential privacy in edge computing[J]. Computer Science, 2024, 51(S1): 896-904.
孙剑明, 赵梦鑫. 边缘计算下差分隐私的应用研究综述[J]. 计算机科学, 2024, 51(S1): 896-904.

[4] DING C, WANG J B, CHENG M, et al. Dynamic transmission and computation resource optimization for dense LEO satellite assisted mobile-edge computing[J]. IEEE Transactions on Communications, 2023, 71(5): 3087-3102.

[5] QI Z B, DU L, HUO R, et al. Muti-camera video collaborative analsis method based on edge computing[J]. Journal on Communications, 2023, 44(8): 14-26.
期治博, 杜磊, 霍如, 等. 基于边缘计算的多摄像头视频协同分析方法[J]. 通信学报, 2023, 44(8): 14-26.

- [6] LUAN L, PAN L W, YAN L, et al. Research on intelligent control technology of accurate cost for unit confirmation in alllinks of power transmission and transformation project based on edge computing[J]. Computer Science, 2021, 48(S2): 688-692.
梁凌, 潘连武, 闫雷, 等. 基于边缘计算的输变电工程全环节单元确认的精准造价智能管控技术研究[J]. 计算机科学, 2021, 48(S2): 688-692.
- [7] BARTHÉLEMY J, VERSTAEVEL N, FOREHEAD H, et al. Edge-computing video analytics for real-time traffic monitoring in a smart city[J]. Sensors, 2019, 19(9): 2048.
- [8] EL-SAYED H, CHAQFEH M. Exploiting mobile edge computing for enhancing vehicular applications in smart cities[J]. Sensors, 2019, 19(5): 1073.
- [9] WANG Z, WANG Y, MUHAMMAD K. Network car hailing pricing model optimization in edge computing-based intelligent transportation system[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(11): 13286-13295.
- [10] WEI R, ZHU C H, WANG Y, et al. Efficient task offloading scheme of Internet of Vehicles based on software defined network and mobile edge computing[J]. Application Research of Computers, 2023, 40(6): 1817-1824.
韦睿, 祝长鸿, 王怡, 等. 基于软件定义网络和移动边缘计算的车联网高效任务卸载方案[J]. 计算机应用研究, 2023, 40(6): 1817-1824.
- [11] BELLAVISTA P, FOGLI M, GIANNELLI C, et al. Application-aware network traffic management in MEC-integrated industrial environments[J]. Future Internet, 2023, 15(2): 42.
- [12] ZHANG C, ZHOU G, LI J, et al. A multi-access edge computing enabled framework for the construction of a knowledge-sharing intelligent machine tool swarm in Industry 4.0[J]. Journal of Manufacturing Systems, 2023, 66: 56-70.
- [13] TAN B, ZHAO S Y, WU J, et al. Virtual reality compressing and transmitting system based on mobile edge computing[J]. Journal on Communications, 2020, 41(4): 45-53.
谭彬, 赵嵩源, 吴俊, 等. 基于移动边缘计算的虚拟现实压缩与传输系统[J]. 通信学报, 2020, 41(4): 45-53.
- [14] ZHOU P, ZHANG W, BRAUD T, et al. Enhanced augmented reality applications in vehicle-to-edge networks[C]//Paris: Proceedings of the 2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops, 2019.
- [15] CHUANG S M, CHEN C S, WU E H K. The implementation of interactive VR application and caching strategy design on mobile edge computing (MEC)[J]. Electronics, 2023, 12(12): 2700.
- [16] AFOLABI I, TALEB T, SAMDANIS K, et al. Network slicing and softwarization: a survey on principles, enabling technologies, and solutions[J]. IEEE Communications Surveys & Tutorials, 2018, 20(3): 2429-2453.
- [17] VON S R, VAN N J. From information security to cyber security[J]. Computers & Security, 2013, 38: 97-102.
- [18] SCHATZ D, BASHROUSH R, WALL J. Towards a more representative definition of cyber security[J]. Journal of Digital Forensics, Security and Law, 2017, 12(2): 8.
- [19] GEENG C, HARRIS M, REDMILES E, et al. "Like lesbians walking the perimeter": experiences of {US}. {LGBTQ+} folks with online security, safety, and privacy advice[C]//Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), 2022: 305-322.
- [20] HANEY J, ACAR Y, FURMAN S. "It's the company, the government, you and i": user perceptions of responsibility for smart home privacy and security[C]//Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), 2021: 411-428.
- [21] HE X, JIN R, DAI H. Deep PDS-learning for privacy-aware offloading in MEC-enabled IoT[J]. IEEE Internet of Things Journal, 2018, 6(3): 4547-4555.
- [22] HALLYBURTON R S, LIU Y, CAO Y, et al. Security analysis of {Camera-LiDAR} fusion against {Black-Box} attacks on autonomous vehicles[C]//Boston: Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), 2022.
- [23] DING W, HU H, CHENG L. IoTSafe: enforcing safety and security policy with real IoT physical interaction discovery[C]//San Diego: Proceedings of the Network and Distributed System Security Symposium, 2021.
- [24] FANG C, NAZARI N, OMIDI B, et al. HeteroScore: evaluating and mitigating cloud security threats brought by heterogeneity[C]//San Diego: Proceedings of the the Network and Distributed System Security Symposium, 2023.
- [25] YUAN B, YANG M, XU Z, et al. Leakage of authorization-data in IoT device sharing: new attacks and countermeasure[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 3196-3210.
- [26] CHEN J, YIN X. Traceable and revocable ciphertext-policy attribute-based encryption scheme based on cloud-fog computing[J]. Journal of Computer Applications, 2021, 41(6): 1611.
- [27] WANG F, CUI J, ZHANG Q, et al. Blockchain-based lightweight message authentication for edge-assisted cross-domain industrial Internet of Things[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 1587-1604.
- [28] GILSENAN C, SHAKIR F, ALOMAR N, et al. Security and privacy failures in popular {2FA} Apps[C]//Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), 2023: 2079-2096.
- [29] MIAO Y, YANG Y, LI X, et al. Efficient privacy-preserving spatial range query over outsourced encrypted data[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 3921-3933.
- [30] TUAN N N, HUNG P H, NGHIA N D, et al. A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN[J]. Electronics, 2020, 9(3): 413.
- [31] LIU Y H, FANG W Y, GUO W Z, et al. Federated incremental learning based DDoS attack detection model in SDN environment[J]. Chinese Journal of Computers, 2024, 47(12): 2852-2866.
刘延华, 方文昱, 郭文忠, 等. 基于联邦增量学习的SDN环境下DDoS攻击检测模型[J]. 计算机学报, 2024, 47(12): 2852-2866.
- [32] BHUSHAN K, GUPTA B B. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment[J]. Journal of Ambient Intelligence and Humanized Computing, 2019, 10: 1985-1997.
- [33] FU C, LI Q, SHEN M, et al. Detecting tunneled flooding traffic via deep semantic analysis of packet length patterns[C]//Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, 2024: 3659-3673.
- [34] QU Z, DUAN R, HAN X, et al. Guessing on dominant paths: understanding the limitation of wireless authentication using channel state information[C]//San Francisco: Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP), 2024.
- [35] SASDRICH P, MORADI A, GüNEYSU T. Hiding higher-order side-channel leakage: randomizing cryptographic implementations in reconfig-

- urable hardware[C]//San Francisco:Proceedings of the Topics in Cryptology-CT-RSA 2017: The Cryptographers' Track at the RSA Conference, 2017.
- [36] SEDJELMACI H, S-MSENOUCI, ANSARI N, et al. A trusted hybrid learning approach to secure edge computing [J]. IEEE Consumer Electronics Magazine, 2021, 11(3): 30-37.
- [37] GERMAIN K S, KRAUGH F. Channel prediction and transmitter authentication with adversarially-trained recurrent neural networks [J]. IEEE Open Journal of the Communications Society, 2021, 2: 964-974.
- [38] XUE J B, DOU J, WANG T, et al. Scheme for maximizing secure communication capacity in UAV-assisted edge computing networks [J]. Computer Science, 2024, 51(S1): 961-967.
薛建彬, 豆俊, 王涛, 等. 无人机辅助边缘计算安全通信能力最大化方案 [J]. 计算机科学, 2024, 51(S1): 961-967.
- [39] YANG Z B, WANG J, MA C J, et al. Python sandbox escape defense mechanism based on third-party library isolation [J]. Netinfo Security, 2024, 24(5): 682-693.
杨志鹏, 王鹏, 马陈军, 等. 基于第三方库隔离的Python沙箱逃逸防御机制 [J]. 信息安全, 2024, 24(5): 682-693.
- [40] DONG F, ZHOU P X. Multi-level immune intrusion detection model for cloud computing [J]. Computer Engineering and Applications, 2016, 52(21): 101-104, 174.
董峰, 周鹏旭. 面向云计算平台的多层免疫入侵检测模型 [J]. 计算机工程与应用, 2016, 52(21): 101-104, 174.
- [41] MOON D, IM H, KIM I, et al. DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks [J]. The Journal of Supercomputing, 2017, 73: 2881-2895.
- [42] FAN W, PENG C, ZHU D L, et al. Research on intrusion response strategy based on static Bayesian game in mobile edge computing network [J]. Journal on Communications, 2023, 44(2): 70-81.
范伟, 彭诚, 朱大立, 等. 移动边缘计算网络下基于静态贝叶斯博弈的入侵响应策略研究 [J]. 通信学报, 2023, 44(2): 70-81.
- [43] ABDAOUI A, ERBAD A, AL-ALI A K, et al. Fuzzy elliptic curve cryptography for authentication in Internet of Things [J]. IEEE Internet of Things Journal, 2021, 9(12): 9987-9998.
- [44] GAO Y Y, ZHANG J N, WANG G, et al. Optimization for GPU-based elliptic curve library and related algorithms [J]. Journal of Cyber Security, 2024, 9(6): 1-16.
高钰洋, 张健宁, 王刚, 等. 基于GPU的椭圆曲线运算库及相关算法优化 [J]. 信息安全学报, 2024, 9(6): 1-16.
- [45] KISHORE R, IOANNOU I, CHRISTOPHOROU C, et al. A security protocol for D2D communications in 5G networks using elliptic curve cryptography [J]. International Journal of Information Security, 2022, 21(6): 1389-1408.
- [46] YIN L, CHEN Y J. Simulation of digital information security transmission in computer rooms based on present algorithm [J]. Computer Simulation, 2023, 40(12): 300-303, 347.
殷莉, 陈益均. Present算法下机房数字化信息安全传输仿真 [J]. 计算机仿真, 2023, 40(12): 300-303, 347.
- [47] SLEEM L, COUTURIER R. Speck-R: an ultra light-weight cryptographic scheme for Internet of Things [J]. Multimedia Tools and Applications, 2021, 80(11): 17067-17102.
- [48] ALTAIE R H, HOOMOD H K. Hybrid SPECK encryption algorithm for Internet of Thing (IoT) [C]//Proceedings of the International Conference of Reliable Information and Communication Technology, 2023: 317-326.
- [49] LIU Y, XING X, TONG Z, et al. Secure and scalable cross-domain data sharing in zero-trust cloud-edge-end environment based on sharding blockchain [J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 2603-2618.
- [50] DOU H, DAN Z, XU P, et al. Dynamic searchable symmetric encryption with strong security and robustness [J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 2370-2384.
- [51] YANG N, TANG C, ZHOU Q, et al. Dynamic consensus committee-based for secure data sharing with authorized multi-receiver searchable encryption [J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 5186-5199.
- [52] RANA M, MAMUN Q, ISLAM R. Balancing security and efficiency: a power consumption analysis of a lightweight block cipher [J]. Electronics, 2024, 13(21): 4325.
- [53] GUO Y, LI L, LIU B. Shadow: a lightweight block cipher for IoT nodes [J]. IEEE Internet of Things Journal, 2021, 8(16): 13014-13023.
- [54] LI G. Data encryption of big data redundancy elimination algorithm combining bloom filter technology [C]//Zhangjiajie: Proceedings of the 2020 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), 2020.
- [55] ROY S, ROY S, BISWAS A, et al. LCB: light cipher block an ultrafast lightweight block cipher for resource constrained IOT security applications [J]. KSII Transactions on Internet and Information Systems (TIIS), 2021, 15(11): 4122-4144.
- [56] YE M, SHEN W, ZHANG J, et al. Securereid: privacy-preserving anonymization for person re-identification [J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 2840-2853.
- [57] TANG X J, MA Y, YU J C, et al. A HEVE information hiding algorithm based on motion vector modification minimizing the distortion between blocks [J]. Journal of Cyber Security, 2024, 9(4): 139-149.
唐小晶, 马熠, 余建昌, 等. 基于运动向量修改的保持块间扰动最小的HEVC信息隐藏算法 [J]. 信息安全学报, 2024, 9(4): 139-149.
- [58] HAN X, TIAN D, DUAN X, et al. A dual mode privacy-preserving scheme enabled secure and anonymous for edge computing assisted Internet of Vehicle networks [C]//Proceedings of the Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, 2021: 65-70.
- [59] LI G, WU H, WU J, et al. Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain [J]. Journal of Cloud Computing, 2024, 13(1): 97.
- [60] LIU W, ZHANG Y, YANG H, et al. A survey on differential privacy for medical data analysis [J]. Annals of Data Science, 2024, 11(2): 733-747.
- [61] CAI J, LIU X, YE Q, et al. A federated learning framework based on differentially private continuous data release [J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(5): 4879-4894.
- [62] ZHENG Z, WANG T, BASHIR A K, et al. A decentralized mechanism based on differential privacy for privacy-preserving computation in smart grid [J]. IEEE Transactions on Computers, 2021, 71(11): 2915-1926.
- [63] WANG K, WANG Y, LIU J Y, et al. Graph convolutional collaborative filtering recommendation algorithm based on Rényi differential privacy [J]. Journal of Software, 2025, 36(3): 1202-1217.
王锐, 王永, 刘金源, 等. 基于Rényi差分隐私的图卷积协同过滤推荐算法 [J]. 软件学报, 2025, 36(3): 1202-1217.
- [64] KONG W, MEDINA A M, RIBERO M, et al. DP-Auditorium: a large scale library for auditing differential privacy [C]//San Francisco: Proceedings of the 2024 IEEE Symposium on Security and Privacy, 2024.

- [65] ZHANG Y, WEI X, CAO J, et al. Blockchain-enabled decentralized attribute-based access control with policy hiding for smart healthcare [J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(10): 8350-8361.
- [66] ZHOU Q, WEI K J, CHEN M H, et al. Blockchain-based domestic cryptographic lightweight attribute-based access control scheme [J]. Journal of Cryptologic Research, 2024, 11(5): 1126-1138.
周权, 卫凯俊, 陈民辉, 等. 基于区块链的国密轻量级属性基访问控制方案 [J]. 密码学报(中英文), 2024, 11(5): 1126-1138.
- [67] WEI Y, GAI K, YU J, et al. Trustworthy access control for multi-access edge computing in blockchain-assisted 6G systems [J]. IEEE Transactions on Industrial Informatics, 2024, 20(5): 7732-7743.
- [68] SHAN D B, DU X H, WANG W J, et al. A scene-aware access control model [J]. Journal of Network and Information Security, 2024, 10(1): 58-78.
单隼斌, 杜学绘, 王文娟, 等. 基于场景感知的访问控制模型 [J]. 网络与信息安全学报, 2024, 10(1): 58-78.
- [69] GE Y, ZHU Q. Gazeta: game-theoretic zero-trust authentication for defense against lateral movement in 5g IOT networks [J]. IEEE Transactions on Information Forensics and Security, 2023, 19: 540-554.
- [70] ZHAO C, ZHAO S, ZHAO M, et al. Secure multi-party computation: theory, practice and applications [J]. Information Sciences, 2019, 476: 357-372.
- [71] BRÜGGEMANN A, SCHICK O, SCHNEIDER T, et al. Don't eject the impostor: fast three-party computation with a known cheater [C]//San Francisco: Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP), 2024.
- [72] AKAMA K, NAKATSUKA Y, SATO M, et al. Scrappy: secure rate assuring protocol with privacy [DB/OL]. <https://arxiv.org/abs/2312.00989>.
- [73] JIANG H, LI J, ZHAO P, et al. Location privacy-preserving mechanisms in location-based services: a comprehensive survey [J]. ACM Computing Surveys (CSUR), 2021, 54(1): 1-36.
- [74] RUAN H F, LI R, LUO K L. Personal data privacy protection method based on vertical partitioning [J]. Chinese Journal of Network and Information Security, 2024, 10(5): 175-187.
阮华锋, 李睿, 罗凯伦. 基于垂直分割的个人数据隐私保护方法 [J]. 网络与信息安全学报, 2024, 10(5): 175-187.
- [75] XU Y, ZHANG H, LI X, et al. Trusted collaboration for MEC-enabled VR video streaming: a multi-agent reinforcement learning approach [J]. IEEE Transactions on Vehicular Technology, 2023, 72(9): 12167-12180.
- [76] RUPANETTI D, KAABOUC N. Combining edge computing-assisted Internet of Things security with artificial intelligence: applications, challenges, and opportunities [J]. Applied Sciences, 2024, 14(16): 7104.
- [77] ARP D, QUIRING E, PENDLEBURY F, et al. Dos and don'ts of machine learning in computer security [DB/OL]. <https://arxiv.org/abs/2010.09470>.
- [78] AZHARI R, SALSABILA A N. Analyzing the impact of quantum computing on current encryption techniques [J]. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 2024, 5(2): 148-157.
- [79] XU C, ERATA F, SZEFER J. Exploration of power side-channel vulnerabilities in quantum computer controllers [C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2023: 579-593.
- [80] GROSSE K, BIERINGER L, BESOLD T R, et al. Towards more practical threat models in artificial intelligence security [DB/OL]. <https://arxiv.org/abs/2311.09994>.
- [81] SHEN J, ZHOU T, HE D, et al. Block design-based key agreement for group data sharing in cloud computing [J]. IEEE Transactions on Dependable and Secure Computing, 2017, 16(6): 996-1010.
- [82] TRUONG N B, SUN K, LEE G M, et al. Gdpr-compliant personal data management: a blockchain-based solution [J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 1746-1761.
- [83] GUAN J, FANG W, HUANG M, et al. Detecting violations of differential privacy for quantum algorithms [DB/OL]. <https://arxiv.org/abs/2309.04819>.
- [84] HE C, MA X, ZHU B B, et al. DorPatch: distributed and occlusion-robust adversarial patch to evade certifiable defenses [C]//San Diego: Network and Distributed System Security Symposium, 2024.
- [85] SU Y, LI D, CHEN L, et al. dRR: a decentralized, scalable, and auditable architecture for rpki repository [C]//San Diego: Network and Distributed System Security Symposium, 2024.

(责任编辑:尹晨茹)