综述

智慧边缘计算安全综述

安星硕[1]，曹桂兴[2]，苗莉[1]，任术波[2]，林福宏[1]
（1. 北京科技大学，北京 100083；2. 中国空间技术研究院，北京 100094）

摘　要：边缘计算将传统的云服务扩展到网络边缘，更贴近用户，适用于具有低时延需求的网络服务。随着边缘计算范式的兴起，其安全问题也得到越来越多的关注。首先介绍了边缘计算范式的基本概念、系统架构以及与其他计算范式的关系。然后分析了当前边缘计算中存在的安全威胁，并针对各种安全威胁探讨了相应的安全技术问题。最后对边缘计算安全技术中关键的入侵检测、访问控制、防御策略、密钥管理技术进行了分析，并提出了进一步研究方向。

关键词：边缘计算；安全技术；系统框架
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2018181

Security of intelligent edge computing: a’survey

AN Xingshuo[1], CAO Guixing[2], MIAO Li[1], REN Shubo[2], LIN Fuhong[1]
1. University of Science and Technology Beijing, Beijing 100083, China
2. China Institute of Space Technology, Beijing 100094, China

Abstract: With the rise of edge computing, more and more attentions have been paid to security issues of edge computing. The basic concepts, system architecture, and the relationship between edge computing and other computing paradigms were introduced. Then the security threats to edge computing were analyzed, and the security technology of edge computing was discussed for these security threats. Finally, the technologies of intrusion detection, access control, defense strategy and key management in edge computing were summarized and the further research directions were pointed out.

Key words: edge computing, security technology, system framework

1　引言

随着大数据与物联网技术的深入发展和广泛应用，接入网络的用户设备数量激增，终端产生的数据呈几何式增长趋势。对分散的计算资源进行数据过滤和处理，将是物联网应用新的重要发

收稿日期：2018−04−05；修回日期：2018−05−09
通信作者：林福宏，FHLin@ustb.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2017YFC0820700）；信息保障技术重点实验室开放基金资助项目（No.KJ-17-101）；国家自然科学基金资助项目（No.61501026）
Foundation Items: The National Key R&D Program of China (No.2017YFC0820700), Foundation of Science and Technology on Information Assurance Laboratory(No.KJ-17-101), The National Natural Science Foundation Project of P. R. China (No. 61501026)

展方向[1]。传统的云计算网络架构可以提供资源集中式远程服务，但当数据服务量急剧加大时，无法满足异构、低时延、密集化的网络接入和服务需求。因此，如何有效地利用分散的计算资源，在网络边缘端执行数据处理任务将成为物联网发展的关键挑战。边缘计算正是为满足这种计算需求而被提出[2]，其有效降低了云数据中心的网络带宽和计算负载，边缘计算模型受到学术界和产业界的广泛关注。

边缘计算是在用户层和数据中心之间的边缘服务器上构建的服务和应用，它将用户层和数据中心的部分功能迁移过来，并提供有限的分布式计算、存储和网络服务。边缘计算作为物联网和云计算的媒介，能够解决物联网和云计算结合引起的终端节点请求时延、云服务器存储和计算负担过重、网络传输带宽压力过大等问题。边缘计算将云计算的服务资源扩展到了网络的边缘，解决了云计算移动性差、地理信息感知弱、时延高等问题。然而，边缘计算兴起的同时也给边缘计算网络中的用户、边缘节点、云服务器的安全防护带来了新的挑战。

2 基本概念及架构

早在 2003 年，AKMAAI 与 IBM 在一份内部研究项目报告《开发边缘计算应用》[3]中提出“边缘计算”的目的，并通过 AKAMAI 与 IBM 在其 Web Sphere 上提供基于边缘的服务。2004 年，Pang [4]在第 20 届 IEEE 国际会议上首次在公开文献中提出边缘计算，提到了“边缘计算是为了实现可扩展且高可用的 Web 服务，将推动企业的逻辑与数据处理中心到代理服务的边缘侧，其优势在于应用程序在边缘侧的运行削减了网络时延，并产生更快的 Web 服务响应”。

现有研究一般将边缘计算的体系架构从网络中央到网络边缘分为 3 层：云计算层、边缘计算层和终端层，如图 1 所示[5-7]。不同层之间一般是根据其计算和存储能力进行划分，终端层、边缘计算层和云计算层三者的计算和存储能力依次增加。为了实现层内和跨层通信，可以采用各种通信技术将每个实体连接起来，包括有线通信（如以太网、光纤）、无线通信（如蓝牙、LTE、ZigBee、NFC、IEEE802.11a/b/c/g/c、卫星链路）或两种技术相结合[8]。边缘计算通过引入位于终端设备和云之间的边缘层，将云服务扩展到了网络边缘。接下来简要介绍边缘计算体系架构每层的组成和功能。

（1）终端层

终端层是最接近终端用户和物理环境的一层，它由各种物联网设备组成。物联网设备分为两种：移动 IoT 设备和固定 IoT 设备。移动 IoT 设备包括可穿戴设备（如健身追踪器、可穿戴照相机和运动手镯等）和移动智能设备（如智能手机、智能手表、智能眼镜、车辆等）。通过个体携带，所有属于同一个人的设备可以使用无线 Ad Hoc 网络相互通信；固定 IoT 设备包括传感器和 RFID 标签等，其被预先部署在特定区域或具体产品上，用以完成预先定义的任务（如产品跟踪、森林火灾探测和控制质量监测）。特别地，某些物联网设备，比如智能手机、车辆等有计算能力，在这里只将其用作智能传感设备，这些设备在地理上分布广泛，负责传感物理特征数据对象或事件，并将这些感测数据传输到上层进行处理和存储。因此，终端层的主要职责是收集原始数据，并报告给上层。比如，在建设智能城市过程中，要在城市周围安装许多固定和移动 IoT 设备，它们之间互相连接，收集城市各个方面的数据。

（2）边缘计算层

边缘计算层层位于网络的边缘，由大量的边缘节点组成，这些边缘节点包括网络设备（如路由器、网关、接入点、基站等）和特定的边缘服务器等（愿意贡献资源的移动设备，包括手机、车辆等）。这些边缘节点广泛分布在终端设备和

云端之间，如咖啡馆、购物中心、公交总站、街道、公园等。边缘节点可以被部署在网络连接中的任何地方，如智能电话中、工厂地板上、路边单元中、车辆中或电线杆顶部。它们能够对收到的感知数据进行计算、传输和临时存储。由于这些边缘节点距离设备仅有一个或两个跳数，因此，实时分析和对时延较为敏感的应用可以在边缘计算层执行。此外，边缘节点也可通过 IP 核心网络与云数据中心连接，并负责与云交互、合作以获得更强大的计算和存储功能。该层旨在将云计算扩展到网络边缘，它具有一定的计算和存储能力。边缘计算层负责定期向云层发送数据，能够提供数据缓存、本地化计算和无线接入三大主要功能，满足移动设备的低时延和高流量需求。

（3）云计算层

云计算层位于整个网络的中心，是一个统一的计算和存储平台[9]。该层由多个高性能服务器和存储设备组成，能够处理和存储大规模的数据，并提供各种应用服务，如智能家居、智能交通、智能工厂等。云计算层负责永久性、大规模的数据存储和全球数据集的全面计算分析。云计算层拥有海量的存储空间和计算资源，只要用户的设备能联网，便可在任何时间、任何地点访问。它采用虚拟化技术将不同用户的数据和 IoT 应用隔离开，因此，这些应用可独立地同时向不同用户提供不同服务。云计算层从各个边缘节点接收数据汇总，并对边缘节点提交的数据和其他来源的数据进行全局分析。此外，云计算层还向边缘层发送策略，以提高边缘节点提供的延迟敏感服务的质量。

另外还有几个与边缘计算相似的范式被相继提出：2009 年，移动云计算[10]（mobile cloud computing，MCC）首次被提出，移动云计算主要集中在“移动授权”的概念上：由于移动设备的可用资源有限，应该委托批量数据的存储和对远程实体执行计算密集型任务。2011 年，思科公司提出了一种新型的计算范式——雾计算（fog computing）[11]。该模式将云端的一些核心功能迁移至网络边缘，从而克服云计算的缺陷，以解决物联网在

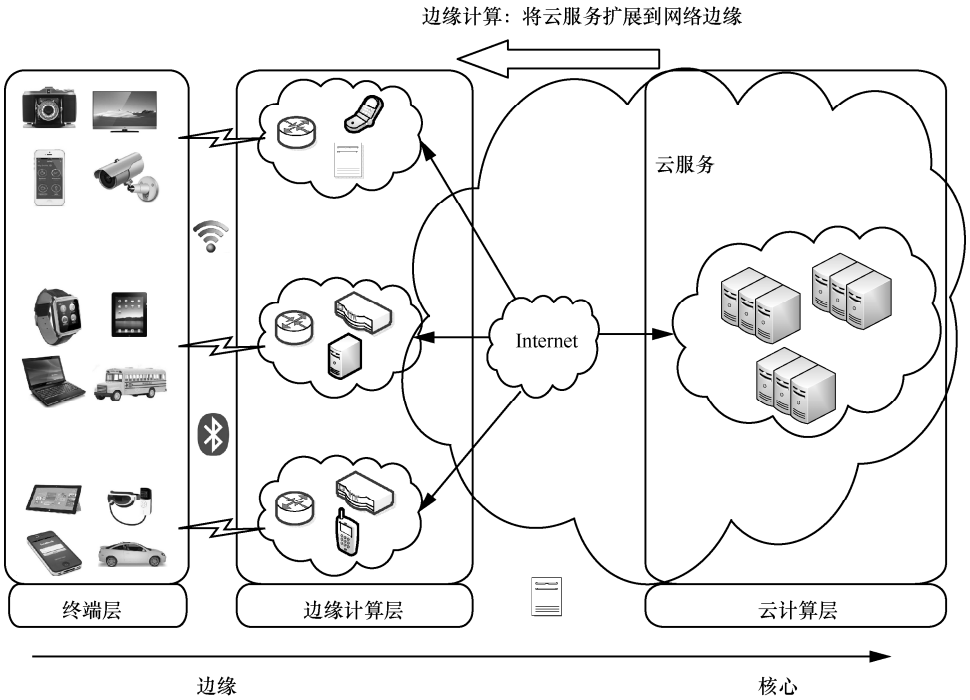


图 1　边缘计算网络结构

传统云计算中遇到的难题。思科认为，雾计算是一种在终端设备和传统云服务器之间提供计算、存储和网络服务的高度虚拟化平台[12]。2014 年，欧洲电信标准协会（European Telecommunications Standards Institute，ETSI）首次给出了基于移动端的边缘计算的标准化概念：移动边缘计算（mobile edge computing，MEC）是在靠近移动用户的无线接入网（radio access network，RAN）内提供 IT 和云计算能力的一种新型的计算方式。

实际上，人们认为边缘计算概念覆盖了较广泛的计算概念，如移动云计算[13]、Cloudlet[14]和雾计算[15-18]。这些计算技术的共同目标是从位于用户地理位置附近的服务器获取服务。一般来说，这种计算模式对时间敏感的应用程序或者没有云介入时具有明显的优势，对于移动设备而言，在边缘执行应用程序或部分应用程序也具有显著的优势。此外，边缘计算提供的传输时延低于云计算，因为移动终端在边缘计算中不会遇到广域网时延问题[19]。对于几种范式的异同之处，有参考文献做过相关的研究[20]，本文也在此基础上进行比较与分析。

从技术角度看，MEC 和 MCC 被认为是云计算和边缘计算的潜在扩展。MEC 作为一种以边缘为中心的计算模式，被认为是现代研究蜂窝基站的关键因素之一。MEC 不仅能够提供边缘服务器和蜂窝基站联合运行[21]，而且可以连接或不连接云数据中心，旨在灵活地访问无线网络信息，用于内容分发和应用程序开发[22]，因此，与终端设备连接在一起，MEC 支持网络中 2 或 3 层的应用程序部署[23-24]。此外，MEC 的目标是为用户提供自适应的更快的蜂窝服务以及提高网络利用效率。近来，MEC 已经取得重大进展，可以支持 5G 通信[25]。

根据参考文献[20]描述：随着物联网的深入应用和智能终端的大量普及，大量用户设备接入网络，需要执行计算任务。然而对于大部分的物联网设备和终端而言，其计算资源、存储资源受限[26]。在资源受限严重的情况下，执行计算密集型应用程序比在本地执行应用程序更为可行。而 MCC 就是为应对这样的挑战而产生的。MCC 支持在更接近最终用户的情况下远程执行流动的移动应用程序[27-28]。在 MCC 中，Cloudlet 的轻量级云服务器都放置在边缘网络中，与终端移动设备和云数据中心链接在一起，Cloudlet 为大量的移动应用程序开发了一个 3 级的应用程序部署平台[29]。MCC 是云计算，移动计算技术和无线通信技术的有机结合体，它能切实提高移动用户的体验质量（QoE），并为网络运营商和云服务提供商创造新的商机。

雾计算（fog computing）也属于边缘计算的范畴。不过雾计算更强调的是对云服务的扩展，它可以将基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）等基于云的服务扩展到网络边缘。也就是说，在雾计算的范畴中是需要考虑核心网络[30]。位于网络边缘的核心网络组件（如核心路由器、区域服务器和万兆交换机等）可以用来当做作雾计算网络中的服务节点（又称雾节点或雾服务器）。位于网络边缘上的雾节点可以放置在距离物联网设备和传感器比较近的地方。由于物联网设备和传感器密集分布，需要对服务请求进行实时响应，雾节点可以为物联网设备和传感器提供存储和实时计算服务。通过雾计算，许多物联网应用的服务交付时延将在很大程度上降至最低。与边缘计算不同，具体的不同计算范式的计算领域区别如图 2[20]所示。

边缘计算用于弥补云计算大数据分析过程的时延性高、周期性长、网络耗能严重等缺陷，通过与云计算配合为用户提供更加全面的计算存储服务，从而满足智能电网、智慧交通、软件定义网络、智慧医疗、智慧车联网等领域在动态连接、实时业务、数字优化、应用智能、安全与隐私保护等方面的需求[31]。

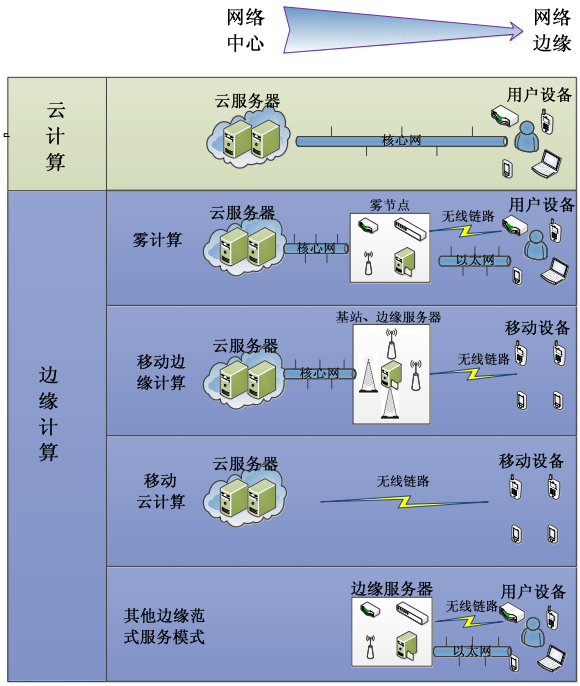


图 2　云计算、雾计算、边缘计算、移动边缘计算以及移动云计算架构之间的区别

3　边缘计算安全威胁

边缘计算是新型的计算范式，针对边缘计算的安全技术问题大多学者从边缘计算结构特征出发，研究边缘计算中面临的安全威胁。Shi 等人[32]提出边缘计算中将面临以下安全问题。

（1）用户对隐私和安全的意识

以 Wi-Fi 网络安全为例，在 4 亿多使用无线连接的家庭中，49%的 Wi-Fi 网络是不安全的，80%的家庭仍然使用默认密码设置他们的路由器。对于公共的 Wi-Fi 热点，89%的热点是不安全的。如果用户没有保护好个人隐私数据，网络摄像头、健康监测仪等设备很容易被他人利用，个人隐私数据被窥探。

（2）边缘设备兼顾数据收集者和所有者

如手机收集的数据将在云服务提供商处存储和分析，而保留边缘数据且让用户拥有是一种较好的隐私数据保护方案。网络边缘设备所收集的数据应存储在边缘，并且用户应有权限制云服务提供商使用这些数据。为保护用户隐私，应在边缘设备中删除高度隐私数据。

（3）数据安全防御有效工具的缺乏

网络边缘设备资源是有限的，现有数据安全保护方法并不能完全适用于边缘计算。而且网络边缘高度动态的环境也会使网络更易受到攻击。为加强对隐私数据的保护，研究人员对隐私保护平台进行了研究，如 Deborah 团队开发的 Open mHealth 平台[33]，以实现对健康数据的标准化处理和存储，但未来的研究仍需要开发更多的工具来处理边缘计算的数据。

此外，互联的节点在传统的无线通信中可能导致系统干扰、嗅探以及其他类型的攻击，在 Ad Hoc 网络和无线传感网络中，这些问题是利用通信加密或者基于通信信道的认证解决。在边缘计算中，数据交换在边缘设备数量和准确性方面要求很高，传统的安全等级不适用于能量有限的边缘设备，而且由于边缘计算中边缘设备部署在网络的边缘，数据发送到资源有限的节点，容易造成信息泄露或者遭到中间人攻击等[34]。因此，需要提出适应于边缘计算环境的防御策略。

边缘计算所面临的威胁与传统数据中心所面临的威胁有相同之处，因为两者共享各种资产（例如服务器、网络基础架构）。除此之外，需要考虑边缘设备的数量、互操作性和移动性、位置感知等其他特征的存在。因此，不仅某些常见威胁的影响将不同（如对边缘数据中心的攻击主要影响与该地理区域相关的服务），还将出现新的威胁。边缘计算安全与传统网络安全的区别总结见表 1[35]。

Roman 等人[36]对边缘计算中可能受到的威胁进行了分类，见表 2。表 2 适合边缘计算中的所有计算范式。如在移动边缘计算中，移动网络运营商不仅控制位于不同地理位置的各种边缘数据中心，而且还控制连接到这些数据中心的核心网络的一部分（即移动网络基础设施）。原则上，基础设施得到很好的维护，具有一致的安全策

表 1　边缘计算环境安全和传统网络安全的区别

安全内容	边缘计算	传统网络安全
安全模式	每个边缘设备都有可能受到攻击	传统网络系统运行在企业内部，对外提供服务接口，利用防火墙和访问控制技术能使网络相对安全
数据存储	数据存放在边缘数据中心	数据存放在内网中，可操作性控制
技术差异	大量采用虚拟化技术	初步虚拟化技术
法律法规	缺少通用标准，法律法规不完善	相关法律标准较完善

略，并能够很好地防止物理和虚拟入侵者，但是，由单一公司管理的大部分服务基础架构也有其缺点：如果一个内部攻击者控制了该基础设施的核心网络，会造成整个系统的崩溃，如果没有很好的应急机制，内部攻击者可能会试图获得更多的特权或利用更多的漏洞，以获得更多收益；另一方面，如果攻击者控制了一个边缘数据中心，就控制了该地理位置边缘数据中心提供的所有服务。此外，对于移动用户而言，终端设备通常会受到恶意软件的攻击、不对等的识别/认证以及 DoS 攻击等影响，而且所有边缘计算都需要支持创建分层的多层架构，其中不同的元素（用户设备、边缘数据中心、核心基础架构）具有不同的角色，这样可以以更集中或更分散的方式来部署某些安全服务（如认证、监视）。

表 2　边缘计算的威胁分类

资产	威胁
网络基础设施	拒绝服务、中间人、流氓网关
边缘数据中心	隐私危害、隐私泄露、特权升级、流氓数据中心、服务操纵
核心基础设施	隐私泄露、服务操纵、流氓基础设施
虚拟基础设施	拒绝服务、资源滥用、隐私泄露、VM 操作
终端用户设备	信息注入、服务操作

针对边缘计算面临的安全问题，相应的防御模型有了初步的研究。Mtibaa 等人[37]在移动边缘计算环境下提出基于 Honey Bot 节点的检测和跟踪算法，利用不安全的 D2D（device-to-device）感染通信通道识别本地的可疑恶意节点并将其隔离。2016 年, Vassilakis 等人[38] 采用攻击性诱骗方法对数据保护进行保护，该方法的思路是：首先监视数据访问以检测任何异常访问模式；其次当怀疑未经授权的访问时，将大量的诱饵信息返回给发送者。实验结果表明，该方案在移动边缘计算环境中对数据能够提供足够的保护。

总之，虽然边缘计算有许多优势，但目前边缘计算安全问题的研究还处于发展阶段，存在许多需要完善的地方，如构建合理的防御策略、传播恶意软件等方面目前还没有相应的研究，因此，为了有效利用终端设备的有限资源以及保护终端用户的数据安全性，需要建立适应边缘计算环境的防御模型。

4　边缘计算安全技术

上文综述了边缘计算的概念以及相关架构，并且对边缘计算范式下的安全威胁做了分析。为应对这些安全威胁，国内外许多学者围绕边缘计算环境下的安全技术问题展开研究。本文从边缘计算网络架构特点出发，从边缘计算环境下入侵检测、访问控制、防御策略和密钥管理 4 个技术角度进行综述，如图 3 所示。

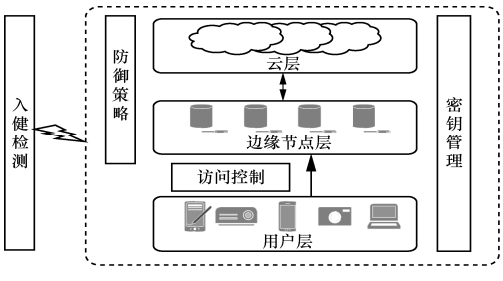


图 3　边缘计算安全技术框架

4.1　边缘计算入侵检测技术

在不同的网络环境下，入侵检测系统

（intrusion detection system，IDS）的检测算法及应用部署有着不同的需求。随着云计算的广泛应用和边缘计算的兴起，很多学者对边缘计算的入侵检测系统进行了广泛研究。

入侵检测主要用来监控和检测主机侧或网络侧的异常数据，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。2010 年 Zhou 等人[39]提出了一种适用于云环境的协作式入侵检测系统，在面对协同攻击时提高了入侵检测的效率。Mazzariello 等人[40]提出了一个在云计算环境中基于网络的入侵检测系统，通过定义一系列的入侵规则来判定入侵行为，该系统在检测外部攻击时具有较高的检测率。为了处理大规模网络数据和应用程序在云中管理控制流量的访问，2011 年 Gul 等人[41]提出一种多线程分布式的入侵检测系统模型。在这个模型中，云计算入侵检测系统能够处理大流量的数据分组，并对其进行分析，有效地生成报表，通过第三方 IDS 检测服务，系统会自动发送安全报告给用户。

物联网、无线传感网络等网络都是边缘计算典型的应用场景。适用于这些应用场景的 IDS 对边缘计算也有借鉴价值。2013 年 Raza 等人[42]提出了一种应用于物联网环境的入侵检测系统 SVELTE，主要针对路由攻击进行检测。2014 年 Shamshirband 等人[43]将 3 人合作策略博弈模型应用于无线传感网络（WSN）的入侵检测中，主要关注 WSN 中的泛洪攻击，通过仿真验证了该模型的攻击检测和防御精度以及能耗和寿命方面都要优于机器学习方法。2015 年肖阳等人[44]引入朋友机制的概念，提出了一种针对移动 Ad Hoc 网络的轻量级入侵检测模型，该模型在检测路由中黑洞攻击时有着良好的性能，检测准确率最高。但他们只针对网络路由层面的攻击进行了仿真实现。然而，要设计一个成熟的能够检测任何网络攻击的检测系统，不能只停留于网络路由层的攻击，需要扩展到链路层、传输层甚至应用层去研究更新的安全威胁和攻击模型来丰富其规则库和网络轮廓，采取渐进的方式不断地对其完善。

2016 年 Hosseinpour 等人[45]提出了一种适用于雾计算的基于人工免疫系统（AIS）的分布式轻量化入侵检测系统。IDS 分布在一个三层的物联网结构中，包括云、雾和边缘层。但是该研究没有对系统的检测率和误报率做深入的分析。2017 年 WANG 等人[46]提出了基于雾设备的协作网络的隐私保护框架，利用该框架设计的入侵检测系统，能在有效地保护隐私数据和网络资源信息安全的前提下，提高检测效率。该项研究重点关注了隐私数据保护，但没有对雾节点资源受限的特点进行研究和分析。2018 年 An 等人[47]提出了一个通用的雾计算 IDS 框架，并在该框架下研究了基于样本筛选极限学习机的雾计算入侵检测分类器模型，提出了一个云、雾混合协作的入侵检测方案，有效地解决了由于雾计算资源有限/雾节点易受攻击等特点所导致的入侵检测效率低、精度差等问题，提高了检测精度和检测效率。Lin 等人[48]在该框架下研究了系统防御资源分配的问题，提出了一个单层优势和最大最小公平分配的策略，将多层次的资源需求层次划分为一系列单层资源需求。通过资源分配来提高入侵检测系统的性能。

4.2　边缘计算访问控制技术

目前关于边缘计算环境下的访问控制技术的研究较少，本文综合对比不同网络环境下的访问控制技术，并提出边缘计算访问控制技术的新需求。2012 年 Pervez 等人[49]提出了一种基于云端数据共享的隐式访问控制策略（oblivious access control policy evaluation，O-ACE）,该策略能够在未向云服务提供商和未经授权的用户揭示有关访问控制策略相关信息的前提下，提供数据访问接口，实现数据的安全共享。2013 年 Yang 等人[50]基于密文策略属性的加密（ciphertext-policy attribute-based encryption，CP-ABE）提出多授权云

存储（data access control for multiauthority cloud storage，DAC-MACS）的数据访问控制，该访问控制策略具有高效的解密和撤销功能，弥补了CP-ABE方案不能直接用于构建多授权云存储系统的数据访问控制方案的不足。2013年Guo等人[51]基于贝叶斯理论，提出了一种安全高效的信任机制，检测访问节点是否是恶意节点，实现安全高效的访问控制。为了提高访问控制的正确性，模型在设计时尽可能多地考虑了受损节点的内部攻击，恶意行为信息通过邻居节点进行收集，并通过父节点对节点的信任值进行计算分析。此外，还基于Diffie-Hellman协议，设计了安全路由的密钥交换协议。但是该方法缺乏在实际的大规模网格系统上进行测试和评估，还不能对访问信任模型的可用性和对整个网格系统运行效率的影响做出准确的评价。2013年Popescu等人[52]指出图像与文字相结合的数据访问控制方式，增加云计算访问接入点级别的安全，该方案避免了简单的用户名和密码认证的缺点，但是用户行为中角色、时态、环境三者之间的约束关系和管理策略问题还有待进一步研究。2013年Jivanadham[53]提出了一种云服务请求者身份验证和授权的访问控制标准。对于注册用户，不需要一个用户名/密码的PKI证书嵌入安全使用平台功能的设备上。不过该方法也存在安全隐患，如果云平台被入侵，攻击者可以通过平台的认证机制，访问主机平台直接得到这些数字文件。2013年Wang等人[54]在协议中引入轻量级同态签名方法，在轻量级同态签名中，每个云计算用户有一套身份属性，并且在他所有的身份属性中计算出一个完整的签名，将其发送给一个可信访问控制服务器，由安全策略服务器验证用户身份属性的完整性签名信息。2013年Zou等人[55]提出一个组密钥认证协议（GKA），该协议具有合理的认证时间，并且减少云中数据流，同时实现了云服务中基于云签名的访问控制，有效拒绝了非法访问。但该方法增加了用户访问服务的时延，影响了用户体验。2013年Ruj等人[56]基于非集中式属性加密方案，提出了一种新的分散式访问控制方案，该方案可防止重播攻击，并支持创建、修改和读取存储在云中的数据，但是该方案需要为未撤销的用户传送密文组件。2013年Wang等人[57]利用云计算通信环境中的匿名身份验证机制可以有效保护用户身份信息，但是该方案的缺陷是不能动态度量用户身份信息。2014年Kim等人[58]提出一种用户动态访问服务器的方案，该方案允许移动用户的云操作权限随位置和时间的改变而自动改变，以增加云接入的安全性。但该方案配置数据庞大、不稳定、占用资源大。2014年Choi等人[59]基于本体推理和语义分析方法，提出Onto-ACM（ontology-based access control model），这是一种语义分析模型，弥补了RBAC（基于角色的访问控制）和C-RBAC（上下文感知RBAC）模型的不足，可以解决服务提供者和用户之间允许访问控制的差异。2015年Xiao等人[60]提出了一种基于属性的访问控制方案，该方案通过评估实体属性（主体和客体）、操作以及请求相关的环境的规则来实现对客体（如文件、应用资源等）的访问控制。不仅能够实现自主访问控制（discretionary access control，DAC）和强制访问控制（mandatory access control，MAC）的功能，还可以实现更细粒度的访问控制。2016年William等人[61]证明了在不受信任的平台上的动态访问控制和加密具有很高的计算成本，提出了一种轻量级的基于身份的公钥加密技术，可用于实现不信任平台的访问控制。2017年Yu等人[62]提出了一种适用于雾计算访问控制的功能性加密（functional encryption，FE）通用框架，该方案除了在雾计算中提供隐私和细粒度访问控制外，还可以保证信道攻击下的雾计算安全性。2017年Fan等人[63]提出了一个可验证的外包多权限访问控制方案，该方案将大部分加密和解密计算都外包给雾设备，并提供了一种高效的用户和属性撤销方法，

能够有效地实现雾计算系统中的数据访问控制，保护数据隐私。

综上所述，不同环境下的访问控制在实际应用中主要存在以下 3 个方面的问题：计算量大、模型复杂、难于重写参数等问题；控制策略混合和冲突的问题；系统工作效率低、性能差，增加了服务时延。由于边缘计算节点分布广泛、资源受限等特点，构建访问控制系统时，应充分考虑边缘计算的特点，并利用其优势，从而提高系统的工作效率、性能。

4.3　边缘计算防御策略

2009 年姜伟等人[64]提出了一种基于攻防随机博弈模型的防御策略选取模型，将攻击者在网络实体上的特权状态作为攻防随机博弈模型的元素,建模网络攻防状态的动态变化，并预测攻击行为和决策最优防御策略。2011 年 Poolsappasit 等人[65]提出了基于成本和收益的多指标量化分析方法，并运用遗传算法计算最优安全策略，使用贝叶斯网络风险管理框架，使系统管理员能够量化各级网络受到攻击的可能性。2011 年 Huang 等人[66]研究了在高度或低度节点上进行有针对性的攻击下相互依存的网络的顽健性，实现了将有针对性的目标攻击转化为相互依赖网络中的随机攻击的技术。2011 年 Gao 等人[67]比较了现有的交互式模型并进行改进，提出了减轻病毒在电子邮件网络中传播的最佳策略，实验表明病毒分布在两个不同的阶段，最有效的免疫策略是节点中介策略。但是，这些研究没有关注分布式攻击应对策略。2012 年 Khouzani 等人[68]提出了一个最优控制模型来评估恶意软件攻击造成的损害最大化问题，从而最大限度地降低了安全补丁的总成本。2013 年吴金宇等人[69]提出了最优弥补集的精确求解算法和近似求解算法，分别应用于小规模攻击图和大规模攻击图，实现了针对不同情况选择不同的求解算法。2017 年 Sun 等人[70]提出了一种在零和多目标博弈中建模网络攻击的方法，该方法结合帕累托最优化和 Q 学习方法来确定最有害的攻击，从而找到最好的防御措施。该方案能够有效地帮助网络管理员找到改进网络安全的切实可行的方法。2017 年 Miao 等人[71]提出为恶意攻击者和防卫者之间的二元交互行为制定一个平均场博弈模型，推导出主动防御行为和被动防御行为的最佳个体策略。

边缘计算防御策略的实质是保护雾设备免遭来自外部的攻击，保护托管在云中的系统、应用程序。传统的安全防御策略没有考虑到攻击者的随机分布或整体网络成本。雾节点具有高密集、分布广泛且资源受限等特点，研究边缘计算环境下的防御策略，需要在考虑网络成本和节点分布广泛的基础上，优化防御算法，降低网络成本，提高防御性能。

4.4　边缘计算密钥管理

密钥管理是用于边缘计算网络中通信过程的加密技术。在边缘计算环境下，由于边缘计算中设备异构性强，网络环境复杂，密钥管理呈现复杂度高、通信开销大等特点。2007 年 Jeong 等人[72]提出了一种传感器网络超图密钥协商方案 KAHG（key agreement protocol for key hypergraph）。在构建的超图模型中，超图的顶点表示通信方，超图的超边表示通信双方的链路。通过使用随机重用技术来构建会话密钥，KAHG 方案可以为超图中所有超边快速建立密钥。KAHG 方案实现了密钥的前向保密性，能够安全防御系统内部攻击。2011 年 Lo 等人[73]提出了一种高效的叶子类层次结构访问控制的密钥分配方案。其中叶级的变化比层级中的非叶级更频繁。该方案基于公钥密码系统和散列函数，由于素数大大减少，节省的存储量显著减少，所提出的方案提供了有价值的效率改进。此外，该方案还可以确保任何未经授权的继任者违反访问政策都无法揭示前任的安全。2011 年 Ding[74]提出了一种基于密钥超图的集中式组密钥管理框架，以最小化密钥存储和组成员密钥更新的开销，并提高可扩展性。2012 年 Shahid 等人[75]提出了轻量级 IKEv2 方案，用于压缩 IPSec 和

IEEE802.15.4 安全的密钥管理，为了解决分布式传感网络的资源约束问题，在 Diffie Hellman 中使用椭圆曲线加密作为非对称加密系统。2014 年 Odelu 等人[76]在 Lo 等人[73]基础上提出了一种新的适用于大型叶级分层结构动态访问控制的密钥管理方案。该方案基于对称密钥密码体制和单向散列函数，与 Lo 等人的方案相比，该方案避免产生大的素数，且该方案用来存储用于大型叶级分级结构中的安全类别的密钥的空间更少。2015 年 Sciancalepore 等人[77]提出了一个面向移动和工业物联网系统的密钥管理协议，该协议提供了顽健的密钥协商、轻量级节点认证、快速重新键控和有效防止中继攻击，并且进行初步的评估，证明其在简单方案中的有效性，为研究边缘计算密钥管理提供了思路。2016 年 Ibrahim[78]指出，由于边缘计算的物理特性，现有的、成熟的网络密钥管理方案并不一定适合边缘计算环境。设计边缘计算专有密钥管理方案时，在保证网络数据安全的基础上，低能耗是考虑的重要因素，如何最大限度地降低密钥管理时的计算、存储以及通信开销是设计的关键。

2017 年，Anzani 等人[79]基于对称设计的混合密钥预分配方法，提出了一个对混合对称设计的改进的方案，提高了连通性和耐用性。2017 年，Daghighi 等人[80]提出一种分级组密钥管理方案，该方案所提出的方案缓解了由移动成员在核心网络引起的 1-affect-*n* 现象、单点故障以及信令负载。支持跨越无线移动环境的成员的移动性。2017 年李治[81]基于超图理论，设计了一种雾计算环境下的组密钥管理方案。针对雾计算覆盖范围广、用户众多的特点，将雾计算划分为两个子网络，并对每个子网的密钥更新方案进行设计。通过对所提密钥管理方案的系统性能分析可知，在保证雾计算密钥管理类方案前向、后向安全的前提下，该方案有效降低了带宽开销和提高了密钥管理方案的可扩展性。

传统的密钥管理方案扩展性能较差，缺少轻量级的实现方法，不适用于具有资源共享、可扩展及虚拟化等特征的边缘计算网络，在保证雾网络安全的前提下，建立适合分布式网络、低开销、高扩展性的密钥管理方案是研究边缘计算网络安全的关键。

5 结束语

边缘计算作为在物联网中被广泛应用的计算范式，将云计算扩展到了网络的边缘，解决了云计算移动性差、地理信息感知弱、时延高等问题以适应于智慧城市环境部署。然而，边缘计算兴起的同时也给边缘计算网络中的用户、边缘节点、云服务器的安全防护带来了新的挑战。一方面，边缘计算位于网络的边缘，更靠近用户，异构的接入环境和多样的业务需求，使得边缘节点面临更复杂的的网络环境。来自用户层和云服务器的攻击都会对整个边缘计算网络带来严重的安全威胁。传统的网络安全技术很难抵御这种多源、跨域、分层的攻击和入侵[82]，需要研究适用于边缘计算范式的网络安全技术来应对新的挑战。另一方面，为了保障边缘计算网络的安全，大部分安全防护技术都需要在边缘节点上进行部署。而边缘计算节点作为分散的、更靠近用户的服务节点，其计算能力和存储能力都不及云服务器。传统的网络安全防护技术通常未考虑系统开销，不适合在边缘计算节点上进行部署。因此异构性、轻量级、分布式，并且适用于边缘计算的安全防护技术和部署方案是今后值得深入研究的课题。

参考文献：

[1] 王计艳, 王晓周, 吴倩,等. 面向 NB-IoT 的核心网业务模型和组网方案[J]. 电信科学, 2017, 33(4): 148-154.
WANG J Y, WANG X Z, WU Q, et al. Core network service model and networking scheme oriented NB-IoT[J]. Telecommunications Science, 2017, 33(4): 148-154.

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

[3] IBM & AKAMAI. Develop edge computing application[EB]. 2003.

[4] PANG H H, TAN K L. Authenticating query results in edge

computing[C]//20th International Conference on Data Engineering,March 30-April 2, 2004, Boston, MA, USA. Piscataway: IEEE Press, 2004: 560 - 571.

[5] GAZIS V, LEONARDI A, MATHIOUDAKIS K, et al. Components of fog computing in an industrial internet of things context[C]//2015 12th Annual IEEE International Conference on Sensing, Communication and Networking-Workshops (SECON Workshops), June 22-25, 2015, Seattle, WA, USA. Piscataway: IEEE Press, 2015: 1-6.

[6] FARUQUE M A A, VATANPARVAR K. Energy management-as-a-service over fog computing platform[J]. IEEE Internet of Things Journal, 2016, 3(2): 161-169.

[7] ZENG D, GU L, GUO S, et al. Joint optimization of task scheduling and image placement in fog computing supported software-defined embedded system[J]. IEEE Transactions on Computers, 2016, 65(12): 3702-3712.

[8] SEHGAL V K, PATRICK A, SONI A, et al. Smart human security framework using internet of things, cloud and fog computing[M]. Berlin: Springer, 2015: 251-263.

[9] 罗萱, 叶通, 金耀辉. 云计算数据中心网络研究综述[J]. 电信科学, 2014, 30(2): 99-104.
LUO X,YE T, JIN Y H, et al. Survey on data center network for cloud computing [J]. Telecommunications Science, 2014, 30(2): 99-104.

[10] DINH H T, LEE C, NIYATO D, et al. A survey of mobile cloud computing: architecture, applications, and approaches[J]. Wireless Communications & Mobile Computing, 2013, 13(18): 1587-1611.

[11] BONOMI F. Connected vehicles, the internet of things, and fog computing[C]//The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Sept 23, 2011, Las Vegas, Nevada, USA. New York: ACM Press, 2011: 13-15.

[12] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the internet of things[C]//The First Edition of the MCC Workshop on Mobile Cloud Computing, August 13-17, 2012, Helsinki, Finland. New York: ACM Press, 2012: 13-16.

[13] GAMLO A H, ZHANG N. Mobile cloud computing: security analysis[C]//2017 IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, April 6-8, 2017, San Francisco, CA, USA. Piscataway: IEEE Press, 2017: 191-198.

[14] SATYANARAYANAN M, LEWIS G, MORRIS E, et al. The role of cloudlets in hostile environments[J]. IEEE Pervasive Computing, 2013, 12(4): 40-49.

[15] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the internet of things[C]//Edition of the MCC Workshop on Mobile Cloud Computing, August 17, 2012, Helsinki, Finland. New York: ACM Press, 2012: 13-16.

[16] ZHANIKEEV M. A cloud visitation platform to facilitate cloud federation and fog computing[J]. Computer, 2015, 48(5): 80-83.

[17] STOJMENOVIC I, WEN S. The fog computing paradigm: Scenarios and security issues[C]//2014 Federated Conference on Computer Science and Information Systems (FedCSIS), Sept 7-10, 2014, Warsaw, Poland.Piscataway: IEEE Press, 2014: 1-8.

[18] DASTJERDI A V, BUYYA R. Fog computing: helping the internet of things realize its potential[J]. Computer, 2016, 49(8): 112-116.

[19] SONMEZ C, OZGOVDE A, ERSOY C. EdgeCloudSim: an environment for performance evaluation of edge computing systems[C]//2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), May 8-11, 2017, Valencia, Spain. Piscataway: IEEE Press, 2017: 39-44.

[20] MAHMUD R, KOTAGIRI R, BUYYA R. Fog computing: A taxonomy, survey and future directions[M]//Internet of everything. Singapore: Springer, 2018: 103-130.

[21] HU Y C, PATEL M, SABELLA D, et al. Mobile edge computing—a key technology towards 5G[R]. 2015, 11(11): 1-16.

[22] CAU E, CORICI M, BELLAVISTA P, et al. Efficient exploitation of mobile edge computing for virtualized 5G in EPC architectures[C]//2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile Cloud), August 8-11, 2016, Beijing, China. Piscataway: IEEE Press, 2016: 100-109.

[23] AHMED A, AHMED E. A survey on mobile edge computing[C]//2016 10th International Conference on Intelligent Systems and Control (ISCO), Jan 6-7, 2016, Coimbatore, Tamilnadu, India. Piscataway: IEEE Press, 2016: 1-8.

[24] KLAS G I. Fog computing and mobile edge cloud gain momentum open fog consortium, ETSI MEC and Cloudlets[EB]. 2015.

[25] RIMAL B P, VAN D P, MAIER M. Mobile edge computing empowered fiber-wireless access networks in the 5G era[J]. IEEE Communications Magazine, 2017, 55(2): 192-200.

[26] MAHMUD M, AFRIN M, RAZZAQUE M, et al. Maximizing quality of experience through context‐aware mobile application scheduling in cloudlet infrastructure[J]. Software: Practice and Experience, 2016, 46(11): 1525-1545.

[27] SANAEI Z, ABOLFAZLI S, GANI A, et al. Heterogeneity in mobile cloud computing: taxonomy and open challenges[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 369-392.

[28] BAHL P, HAN R Y, LI L E, et al. Advancing the state of mobile cloud computing[C]//The Third ACM Workshop on Mobile Cloud Computing and Services, June 25-29, 2012, Low Wood Bay, UK. New York: ACM Press, 2012: 21-28.

[29] ALRAWAIS A, ALHOTHAILY A, HU C, et al. Fog computing for the internet of things: security and privacy issues[J]. IEEE Internet Computing, 2017, 21(2): 34-42.

[30] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the internet of things[C]//The first edition of the MCC Workshop on Mobile Cloud Computing, August 17, 2012, Helsinki, Finland. New York: ACM Press, 2012: 13-16.

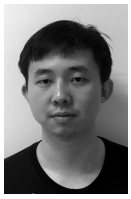
[31] BHARDWAJ K, SHIH M W, AGARWAL P, et al. Fast, scalable and secure onloading of edge functions using AirBox[C]//2016 IEEE/ACM Symposium on Edge Computing (SEC), Oct 27-28, 2016, Seattle, WA, USA. Piscataway: IEEE Press, 2016: 14-27.

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

637-646.
[33] Open mHealth. Open mHealth platform[EB]. 2016.
[34] ESPOSITO C, CASTIGLIONE A, POP F, et al. Challenges of connecting edge and cloud computing: a security and forensic perspective[J]. IEEE Cloud Computing, 2017, 4(2): 13-17.
[35] MACH P, BECVAR Z. Mobile edge computing: a survey on architecture and computation offloading[J]. IEEE Communications Surveys & Tutorials, 2017(99): 1.
[36] ROMAN R, LOPEZ J, MAMBO M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges[J]. Future Generation Computer Systems, 2016, arXiv: 1602.00484.
[37] MTIBAA A, HARRAS K, ALNUWEIRI H. Friend or foe? Detecting and isolating malicious nodes in mobile edge computing platforms[C]//2016 IEEE International Conference on Cloud Computing Technology and Science, Dec 12-15, 2016, Luxembourg City, Luxembourg. Piscataway: IEEE Press, 2016: 42-49.
[38] VASSILAKIS V, CHOCHLIOUROS I P, SPILIOPOULOU A S, et al. Security analysis of mobile edge computing in virtualized small cell networks[C]//2016 IFIP International Conference on Artificial Intelligence Applications and Innovations, Sept 16–18, 2016，Thessaloniki, Greece. Berlin: Springer, 2016: 653-665.
[39] ZHOU C V, LECKIE C, KARUNASEKERA S. A survey of coordinated attacks and collaborative intrusion detection[J]. Computers & Security, 2010, 29(1): 124-140.
[40] MAZZARIELLO C, BIFULCO R, CANONICO R. Integrating a network ids into an open source cloud computing environment[C]//2010 Sixth International Conference on Information Assurance and Security (IAS), June 23-25, 2010, Miyazaki, Japan. Piscataway: IEEE Press, 2010: 265-270.
[41] GUL I, HUSSAIN M. Distributed cloud intrusion detection model[J]. International Journal of Advanced Science and Technology, 2011(34): 71-82.
[42] RAZA S, WALLGREN L, VOIGT T. SVELTE: real-time intrusion detection in the internet of things[J]. Ad Hoc Networks, 2013, 11(8): 2661-2674.
[43] SHAMSHIRBAND S, PATEL A, ANUAR N B, et al. Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks[J]. Engineering Applications of Artificial Intelligence, 2014(32): 228-241.
[44] 肖阳, 白磊, 王仙. 基于朋友机制的移动 Ad Hoc 网络路由入侵检测模型研究[J]. 通信学报, 2015, 36(S1): 203-214.
XIAO Y, BAI L, WANG X. Friends mechanism-based routing intrusion detection model for mobile Ad Hoc network[J]. Journal on Communications, 2015, 36(S1): 203-214.
[45] HOSSEINPOUR F, AMOLI P V, 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 & Its Applications, 2016, 10(5).
[46] WANG Y, XIE L, LI W, et al. A privacy-preserving framework for collaborative intrusion detection networks through fog computing[C]//2017 International Symposium on Cyberspace Safety and Security, October 23-25, 2017, Xi'an, China. Berlin: Springer, 2017: 267-279.
[47] AN X, ZHOU X, XING L, et al. Sample selected extreme learning machine based intrusion detection in fog computing and MEC[J]. Wireless Communications & Mobile Computing, 2018: 1-10.
[48] LIN F H, ZHOU Y T, AN X S, et al. Fair resource allocation in intrusion detection system for edge computing[J]. IEEE Consumer Electronics Magazine (Accepted).
[49] PERVEZ Z, KHATTAK A M, LEE S, et al. Oblivious access control policies for cloud based data sharing systems[J]. Computing, 2012, 94(12): 915-938.
[50] YANG K, JIA X, REN K, et al. DAC-MACS: effective data access control for multiauthority cloud storage systems[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1790-1801.
[51] GUO J W, ZHOU X W, YUAN J L,et al. Secure access control guarding against internal attacks in distributed networks[J]. Wireless Personal Communications, 2013, 68(4): 1595-1609.
[52] POPESCU D E, LONEA A M. An hybrid text-image based authentication for cloud services[J]. International Journal of Computers Communications & Control, 2013, 8(2): 263-274.
[53] JIVANADHAM L B, ISLAM A K M, KATAYAMA Y, et al. Cloud cognitive authenticator (CCA): a public cloud computing authentication mechanism[C]//2013 International Conference on Informatics, Electronics & Vision (ICIEV), May 17-18, 2013, Dhaka, Bangladesh. Piscataway: IEEE Press, 2013: 1-6.
[54] WANG Z, SHA K, LV W. Slight homomorphic signature for access controlling in cloud computing[J]. Wireless personal communications, 2013, 73(1): 51-61.
[55] ZOU B, ZHANG H. Integrity protection and attestation of security critical executions on virtualized platform in cloud computing environment[C]//The 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, August 20-23, 2013, Beijing, China. Piscataway: IEEE Press, 2013: 2071-2075.
[56] RUJ S, STOJMENOVIC M, NAYAK A. Decentralized access control with anonymous authentication of data stored in clouds[J]. IEEE Transactions on Parallel & Distributed Systems, 2013, 25(2): 384-394.
[57] WANG Z, SHA K, LV W. Slight homomorphic signature for access controlling in cloud computing[J]. Wireless Personal Communications, 2013, 73(1): 51-61.
[58] KIM J M, MOON J K. Secure authentication system for hybrid cloud service in mobile communication environments[J]. International Journal of Distributed Sensor Networks, 2014(1): 1-7.
[59] CHOI C, CHOI J, KIM P. Ontology-based access control model for security policy reasoning in cloud computing[J]. Journal of Supercomputing, 2014, 67(3):711-722.
[60] XIAO M, WANG M, LIU X, et al. Efficient distributed access control for big data in clouds[C]//2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),

Mar 25-30, 2012, Orlando, FL, USA. Piscataway: IEEE Press, 2015: 202-207.
[61] GARRISON W C, SHULL A, MYERS S, et al. On the practicality of cryptographically enforcing dynamic access control policies in the cloud[C]//2016 IEEE Symposium on Security and Privacy (SP), May 23-25, 2016, San Jose, CA, USA. Piscataway: IEEE Press, 2016: 819-838.
[62] YU Z, MAN H A, XU Q, et al. Towards leakage-resilient fine-grained access control in fog computing[J]. Future Generation Computer Systems, 2018: 78(1): 763-777.
[63] FAN K, WANG J, WANG X, et al. A secure and verifiable outsourced access control scheme in fog-cloud computing[J]. Sensors, 2017, 17(7): 1695.
[64] 姜伟, 方滨兴, 山志宏, 等. 基于攻防博弈模型的网络安全测评和最主动防御[J]. 计算机学报, 2009, 32(4): 817-827.
JIANG W, FANG B X, SHAN Z H, et al. Evaluating network security and optimal active defense based on attack-defense game model [J]. Chinese Journal of Computers, 2009, 32(4): 817-827.
[65] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using bayesian attack graphs[J]. IEEE Transactions on Dependable & Secure Computing, 2011, 9(1): 61-74.
[66] HUANG X, GAO J, BULDYREV S V, et al. Robustness of interdependent networks under targeted attack[J]. Physical Review E, 2011, 83(6): 065101.
[67] GAO C, LIU J, ZHONG N. Network immunization and virus propagation in email networks: experimental evaluation and analysis[J]. Knowledge and Information Systems, 2011, 27(2): 253-279.
[68] KHOUZANI M H R, SARKAR S, ALTMAN E. Maximum damage malware attack in mobile wireless networks[J]. IEEE/ACM Transactions on Networking (TON), 2012, 20(5): 1347-1360.
[69] 吴金宇. 网络安全风险评估关键技术研究[D]. 北京: 北京邮电大学, 2013.
WU J Y. Research on key technology of network security risk assessment[D]. Beijing: Beijing University of Posts and Telecommunications, 2013.
[70] SUN Y, XIONG W, YAO Z, et al. Network defense strategy selection with reinforcement learning and pareto optimization[J]. Applied Sciences, 2017, 7(11): 1138.
[71] MIAO L, LI S. Cyber security based on mean field game model of the defender: attacker strategies[J]. International Journal of Distributed Sensor Networks, 2017, 13(10): 155014771773790.
[72] JEONG I R, LEE D H. Key agreement for key hypergraph[J]. Computers & Security, 2007, 26(7): 452-458.
[73] LO J W, HWANG M S, LIU C H. An efficient key assignment scheme for access control in a large leaf class hierarchy[J]. Information Sciences, 2011, 181(4): 917-925
[74] DING Y, ZHOU X, CHENG Z, et al. Secure group communications using key hypergraphs[J]. Journal of Computational Information Systems, 2012, 8(12): 5035-5042.
[75] RAZA S, VOIGT T, JUTVIK V. Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security. IETF/IAB workshop on smart object security[EB]. 2012.
[76] ODELU V, DAS A K , GOSWAMI A. A secure effective key management scheme for dynamic access control in a large leaf class hierarchy[J]. Information Sciences, 2014, 269(4): 270-285.
[77] SCIANCALEPORE S, CAPOSSELE A, PIRO G, et al. Key management protocol with implicit certificates for IoT systems[C]//The 2015 Workshop on IoT Challenges in Mobile and Industrial Systems, May 18, 2015, Florence, Italy. New York: ACM Press, 2015.
[78] IBRAHIM M. Octopus: an edge-fog mutual authentication scheme[J]. International Journal of Network Security, 2016, 18(6): 1089-1101.
[79] ANZANI M, JAVADI H H S, MODIRIR V. Key- management scheme for wireless sensor networks based on merging blocks of symmetric design[J]. Wireless Networks, 2017(1): 1-13.
[80] DAGHIGHI B, KIAH M L M, IQBAL S, et al. Host mobility key management in dynamic secure group communication[J]. Wireless Networks, 2017(1): 1-19.
[81] 李治. 雾计算环境下数据安全关键技术研究[D]. 北京: 北京科技大学, 2017.
LI Z. Research on key technology of data security in fog computing environment[D]. Beijing: University of Science and Technology Beijing, 2017.
[82] 王笑帝, 张云勇, 刘锦,等. 云计算虚拟化安全技术研究[J]. 电信科学, 2015, 31(6):1-5.
WANG X D, ZHANG Y Y, LIU D, et al. Research on security of virtualization on cloud computing [J]. Telecommunications Science, 2015, 31(6): 8-12, 24.

[作者简介]:



安星硕（1988−），男，北京科技大学计算机与信息工程学院博士生，主要研究方向为雾计算、网络安全和入侵检测。

曹桂兴（1963−），男，中国空间技术研究院通信卫星事业部研究员，主要研究方向为天基信息产、传输与分发和边缘计算。

苗莉（1986−），女，北京科技大学计算机与信息工程学院博士生，主要研究方向为网络安全、边缘计算安全和平均场博弈。

任术波（1976−），男，博士，中国空间技术研究院通信卫星事业部高级工程师，主要研究方向为移动通信和边缘计算。

林福宏（1981−），男，博士，北京科技大学计算机与信息工程学院副教授，主要研究方向为边缘计算和网络安全。