万物互联背景下的边缘计算安全需求与挑战

Security Requirements and Challenges in Edge Computing for Internet of Everything

马立川/MA Lichuan[1,2]，裴庆祺/PEI Qingqi[1,2]，肖慧子/XIAO Huizi[1,2]

（1. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 西安市移动边缘计算及安全重点实验室，陕西 西安 710071）

(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China;
2. Xi'an Key Laboratory of Mobile Edge Computing and Security, Xi'an 710071, China)

摘要：作为万物互联时代新型的计算模型，边缘计算具有的分布式、“数据第一入口”、计算和存储资源相对有限等特性，使其除了面临信息系统普遍存在网络攻击之外，还不可避免地引入了一些新的安全威胁。为此，从4个方面对边缘计算的安全需求进行阐述，同时对其主要安全技术的设计以及实现所面临的挑战进行分析，较为全面地指出了边缘计算在身份认证、访问控制、入侵检测、隐私保护、密钥管理中存在的具体安全问题。

关键词：万物互联；边缘计算；安全需求；隐私保护

Abstract: As a new computing paradigm in the Internet of Everything, edge computing has the following characteristics: distributed, data first entry, relatively limited of computing and storage resources. These characteristics bring some new security threats and network attacks to the edge computing. In this paper, the security requirements of edge computing are elaborated from four aspects, and the design of its main security technology and the challenges are also analyzed. It comprehensively points out the specific security issues of edge computing in identity authentication, access control, intrusion detection, privacy protection and key management.

Key words: Internet of Everything; edge computing; security requirements; privacy preserving

DOI：10.12142/ZTETJ.201903006
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190612.0847.002.html

网络出版日期：2019-06-12
收稿日期：2018-12-28

1 万物互联背景下从云到边缘的演变

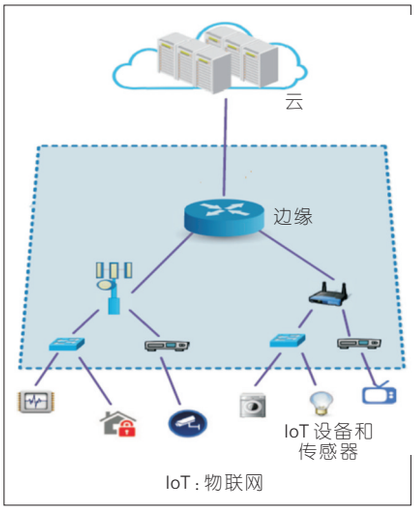
随着单片机嵌入式系统和无线通信技术的发展，物联网技术近年来得到了长足的发展和普及，其实际应用包括智能家居、智慧交通、无人驾驶等。近年来，除了“物”与“物”的互联，还增加了“物”与“人”的互联，其显著特点是“物”端具有更强的计算能力和语境感知能力，将人和信息融入到互联网中，该趋势使得人类社会正在迈入万物互联（IoE）的时代[1]。

万物互联的核心在于收集来自于终端设备的海量数据，利用以大数据、机器学习、深度学习为代表的智能技术，去满足不同行业的业务需求，如制造、交通、医疗、农业等各行各业。在此背景下，所需要连接的终端设备数量达到数十亿甚至数万亿，其产生的数据呈爆炸式增长。到2020年，连接到网络的无线设备数量将达到500亿台，生成的数据量达到507.9 ZB。

目前，海量数据的存储和处理主要依赖于集中式的云计算模型，其特征主要表现为数据和存储均位于部署在偏远地区的云计算中心。尽管云数据中心以堆叠硬件的方式具有较强的计算和存储能力，但是万物互联背景下，网络边缘的终端设备产生的数据已经达到海量级

别，这给云计算模型带来以下挑战：(1)线性增长的集中式云计算能力无法匹配终端所产生数据的指数增长需求[2]；(2)海量数据传输到云计算中心急剧增加了传输带宽的负载量，造成较大的网络时延，这给对时延敏感的应用场景（如无人驾驶、工业制造等）带来了严峻的挑战；(3)终端设备电能有限，数据传输会造成电能消耗较大。为此，集中式的云计算模型已经无法满足万物互联下的海量数据的高效传输以及处理需求。

在此背景下，边缘计算作为一种新的计算模式，架起物联网设备和数据中心之间的桥梁，使数据在源头附近就能得到及时有效地处理。如图1所示的基于物-边缘-云的三层服务交付架构，将从数据源到云计算中心数据路径之间的任意计算、存储、网络资源，形成高度虚拟化平台的“边缘层”为用户提供服务，其中的每层都具有灵活性和可扩展性，可以按需增减相应数量的实体。边缘计算出现之前，微云计算、雾计算和移动边缘计算等几种方法都是利用相似的思想为云计算提供了补充解决方案。根据2018年11月发布的《边缘计算参考架构3.0》所述：边缘计算模型具有分布式、“数据第一入口”、计算和存储资源相对有限等特性。



▲图1 物-边缘-云三层服务交付架构

然而，网络边缘侧更贴近万物互联的终端设备。由于终端设备的开放性和异构性，以及相对有限的计算和存储资源（与云计算中心相比），使得访问控制和防护的广度和难度大幅提升[3]。此外，边缘计算还面临信息系统中普遍存在的网络攻击威胁。为此，跨越云计算和边缘计算之间的纵深，实施端到端的防护，全方位保障边缘计算的安全，增强其抵抗各种安全威胁的能力，是边缘计算促进万物互联进一步发展的前提和必要条件。

2 边缘计算安全需求

安全是指达到抵抗某种安全威胁或安全攻击的能力，横跨云计算和边缘计算，需要实施端到端的防护。万物互联系统在紧密耦合网络系统与物理世界中的关键性作用决定了安全属性和隐私保护的相关需求要比在以往任何信息系统中更加重要。

2.1 边缘计算安全的必要性

万物互联系统中终端设备具有超大规模、低成本设计、资源受限、设备异构等特性。同时，开发商重视功能优于安全的事实、用户更高的隐私要求、更难的信任管理使得保证万物互联系统的安全性显得更具挑战性。

目前，边缘计算面临巨大的安全威胁。文献[4]中，作者分析了2个利用边缘计算应用场景的安全问题。一个是在智能制造工厂的场景下，攻击者可以篡改通信数据包，注入伪造的压力测量值欺骗决策器，延迟控制阀门的动作并造成设备损坏。如果没有适当的安全防范措施，不仅生产过程可能中断，工人的生命在很大程度上受到威胁。另一个则是移动边缘计算中无人机操作的安全问题，可以产生模拟的全球定位系统（GPS）信号误导无人机系统组件，使其驾驶到目标区域以达到捕获的目的。作者用无人机实验验证并达到了在不产生附加损失的情况下友好地捕获了非合作性无人机的目的。

在文献[5]中，华盛顿大学计算机科学与工程系的科研人员对配备智能电子控制系统的典型豪华轿车进行了实验安全分析，发现其安全保护系统具有很多设计时就存在的安全漏洞，同时并不是车上的所有组件都遵循其自己设计的安全协议，这使得实验人员能够轻易地侵入车辆引擎控制模块、电子刹车控制模块等性命攸关的重要车辆控制部件，从而远程控制行驶车辆的油门、刹车等。

2017年6月1日正式生效的《中华人民共和国网络安全法》特别强调了关键信息基础设施的运行安全，而能源、交通、制造等关键基础设施的工业控制环境无疑将是安全建设的重中之重。2016年中国信息通信研究院云计算白皮书指出：

公有云服务提供商向用户提供大量一致化的基础软件(如操作系统、数据库等资源),这些基础软件的漏洞将造成大范围的安全问题与服务隐患。安全已经成为阻碍万物互联和云计算发展的最大因素。

边缘计算是万物互联的延伸和云计算的扩展,三者的有机结合将为万物互联时代的信息处理提供较为完美的软硬件支撑平台,为能源、交通、制造、医疗等行业带来飞跃式发展。而通过边缘设备将类似云计算的功能带到了网络的边缘,可能引入新的安全挑战,一些传统的安全解决方法,例如基于非对称密钥协议和基于网际协议地址(IP)的解决方案,无法有效地应用于边缘计算系统,进而带来了一系列全新的安全需求。

同时,边缘计算可以提供理想的平台来解决物联网中的许多安全和隐私问题。在网络边缘处计算、连接、存储能力的协同使用可以达到万物互联应用的部分安全目的。例如,边缘设备可以作为加密计算的代理或者在公钥基础设施(PKI)技术中协助认证中心(CA)管理证书的发放与撤销,而其下面的物联网设备和传感器就缺乏实现这些操作的必要资源。

综上所述,网络边缘高度动态异构的复杂环境也会使网络难于保护,从而带来新的安全挑战。边缘计算同时又为资源、能量受限的终端设备提供一套全新的安全解决方案。因此,研究边缘计算场景的安全和隐私保护的相关问题是万物互联系统得到进一步发展的首要前提条件。

2.2 边缘计算安全的需求分析

边缘计算安全需求分析如图2所示,按照边缘计算参考架构,主要分为物理安全、网络安全、数据安全和应用安全4个方面的需求。

2.2.1 物理安全需求

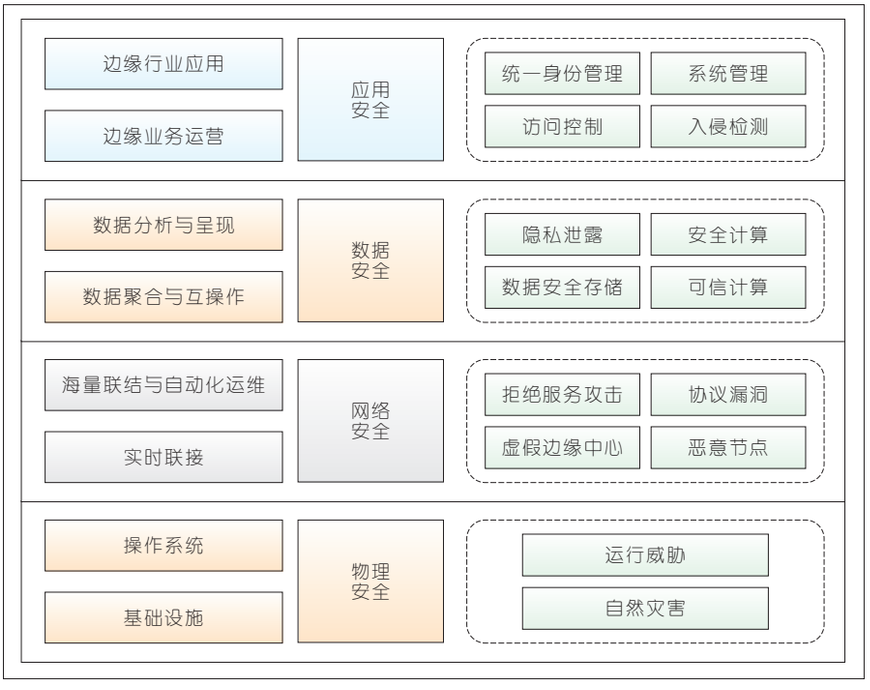
物理安全是保护智能终端设备、设施以及其他媒体避免自然界中不可抗力(如地震、火灾、龙卷风、泥石流)及人为操作失误或错误所造成的设备损毁、链路故障等使边缘计算服务部分或完全中断的情况。物理安全是整个服务系统的前提,物理安全措施是万物互联系统中必要且基础的工作。

对于边缘计算设备来说,其在对外开放的、不可控的甚至人迹罕至的地方运行,所处的环境复杂多样,因此更容易受到自然灾害的威胁。且在运行过程中,由间接或者自身原因导致的安全问题(如能源供应;冷却除尘、设备损耗等),运行威胁虽然没有自然灾害造成的破坏彻底,但是如果缺乏良好的应对手段,仍然会导致灾难性的后果,使得边缘计算的性能下降,服务中断和数据丢失。

2.2.2 网络安全需求

网络安全是指通过采用各种技术和管理措施,使网络系统正常运行,从而确保网络数据的可用性、完整性和保密性,以使系统连续可靠正常地运行,网络服务不中断。

大数据处理背景下,海量终端设备通过网络层实现与边缘设备的数据交互传输,边缘设备可以通过接入网络层实现更加广泛的互联功能。而大量设备的接入,给网络管



▲图2 边缘计算安全需求分析

理带来沉重负担的同时，也增加了边缘设备被攻击的可能性。文献[5-6]中所采用的攻击方式大都是在无线传输途中采用窃听、截获数据包等方法进行流量分析，然后篡改或伪造数据包来达到控制目标的目的。

相较于云计算数据中心，边缘节点的能力有限，更容易被黑客攻击。虽然单个被破坏的边缘节点损害并不大，并且网络有迅速找到附近可替代节点的调度能力；但如果黑客将攻陷的边缘节点作为“肉鸡”去攻击其他服务器，进而会对整个网络造成影响。现有大多安全保护技术计算保护流程复杂，不太适合边缘计算的场景。所以，设计适合于万物互联背景下边缘计算场景中轻量级的安全保护技术是网络安全的重大需求。

2.2.3 数据安全需求

数据信息作为一种资源，具有普遍性、共享性、增值性、可处理性和多效用性，而数据安全的基本目标就是要确保数据的3个安全属性：机密性、完整性和可用性。

要对数据的全生命周期进行管理的同时实现这3个安全属性才能保证数据安全。整个生命周期包括6个阶段[7]：创建，数据的产生和采集过程；存储，数据保存到存储介质的过程；使用，数据被浏览、处理、搜索或进行其他操作的过程；共享，数据在拥有者、合作者、使用者之间交互的过程；存档，极少使用的数据转入长期存储的过程；销毁，不再使用的数据被彻底删除和擦除的过程。

在边缘计算中，用户将数据外包给边缘节点，同时也将数据的控制权移交给边缘节点，这便引入了与云计算相同的安全威胁。首先，很难确保数据的机密性和完整性，因为外包数据可能会丢失或被错误地修改。其次，未经授权的各方可能会滥用上传的数据图谋其他利益。虽然相对于云来说边缘计算已经规避了多跳路由的长距离传输，很大程度地降低了外包风险；但是边缘计算设备部署的应用属于不同的应用服务商，接入网络属于不同的运营商，导致边缘计算中多安全域共存、多种格式数据并存。因此属于边缘计算的数据安全问题也日益突出，如在一个边缘节点为多个用户服务时，如何确保用户数据的安全隔离？在如此复杂多变的环境中，一个边缘节点瘫痪后，如何实现安全快速地迁移数据？当多个边缘节点协同服务时，如何能够在不泄露各自数据的情况下设计多方的协作服务？

另一个万物互联背景下边缘计算的数据安全需求就是用户隐私保护。比起云中心隐私数据泄露的风险，边缘计算设备位于靠近数据源的网络边缘侧，相对于位于核心网络中的云计算数据中心，可以收集更多用户高价值的的敏感信息，包括位置信息、生活习惯、社交关系甚至健康状况等，边缘计算是否会成为商业公司收集用户隐私数据的平台？物联网设备的计算资源难以执行复杂的隐私保护算法，边缘式大数据分析中如何在数据共享时保证用户的隐私？这些问题都将成为边缘计算发展的重要阻碍。

2.2.4 应用安全需求

应用安全，顾名思义就是保障应用程序使用过程和结果的安全。边缘式大数据处理时代，通过将越来越多的应用服务从云计算中心迁移到网络边缘节点，能保证应用得到较短的响应时间和较高的可靠性，同时大大节省网络传输带宽和智能终端电能的消耗。但边缘计算不仅存在信息系统普遍存在的共性应用安全问题，如拒绝服务攻击、越权访问、软件漏洞、权限滥用、身份假冒等，还由于其自身特性存在其他的应用安全的需求。在边缘这种多安全域和接入网络共存的场景下，为保证应用安全，该如何对用户身份进行管理和实现资源的授权访问则变得非常重要。身份认证、访问控制和入侵检测相关技术便是在边缘计算环境下保证应用安全的重点需求。

3 边缘计算安全挑战

通过对边缘计算安全需求的讨论分析可以看出：边缘计算的特性使其在构建安全保护方案时给系统开发人员带来了重大挑战。

3.1 身份认证

身份认证，也称“身份验证”或“身份鉴别”，是验证或确定用户提供的访问凭证是否有效的过程。用户可以是个人、应用或服务，所有的用户都应在被认证后才能访问资源，从而确定该用户是否具有对某种资源的访问和使用权限，使系统

的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

在边缘计算中，不同可信域中的边缘服务器、云服务提供商和用户分别提供和访问实时服务，其分散化、实时服务的低延迟需求和用户的移动性给身份认证的实现带来了巨大的障碍，很难保证所有涉及的实体都是可信的。在访问这些服务之前，应该对每个用户进行身份验证，以确保其真实性和可信性。身份认证应具备的功能包括：一方面应能够在分布式异构网络环境下，使用相关的协议、规范以及技术将分散的身份信息进行集中管理，实现单点登录，也可以方便地扩充跨身份标识域的访问等功能；另一方面应提供友好的体验环境，保护用户隐私，有效地对用户的行为进行审计。

身份认证是终端设备安全的基本要求，许多万物互联设备没有足够的内存和中央处理器（CPU）功率来执行认证协议所需的加密操作。这些资源有限的设备可以将复杂的计算和存储外包给可以执行认证协议的边缘设备，与此同时也会带来一定的问题：终端用户和边缘计算服务器之间必须相互认证，这种多安全域共存的情况下安全凭证从何而来？如何在大量分布式边缘服务器和云计算中心之间实现统一的身份认证和密钥管理机制？万物互联中存在大量的资源受限设备，无法利用传统的PKI体制对边缘计算设备或服务进行认证。边缘计算环境下终端具有很强的移动性，如何实现用户在不同边缘设备切换时的高效认证具有很大挑战[8]。显然，轻量级的身份认证技术是保证边缘计算安全的前提和挑战。

3.2 访问控制

访问控制是基于预定模式和策略对资源的访问过程进行实时控制的技术，按用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用。访问控制的任务是在满足用户最大限度享受资源共享需求的基础上，实现对用户访问权限的管理，防止信息被非授权篡改和滥用，是保证系统安全、保护用户隐私的可靠工具。在万物互的联背景下，需要访问控制以确保只有受信任方才能执行给定的操作，不同用户或终端设备具有访问每个服务的独特权限。

访问控制除了负责对资源访问控制外，还要对访问策略的执行过程进行追踪审计。在边缘计算中，访问控制变得更加艰难，主要原因在于：首先要求边缘计算服务提供商能够在多用户接入环境下提供访问控制功能；其次，访问控制应支持用户基本信息和策略信息的远程提供，还应支持访问控制信息的定期更新；最后，对于高分布式且动态异构数据的访问控制本身就是一个重要的挑战。

3.3 入侵检测

入侵检测通过包括监测、分析、响应和协同等一系列功能，能够发现系统内未授权的网络行为或异常现象，收集违反安全策略的行为并进行统计汇总，从而支持安全审计、进攻识别、分析和统一安全管理决策。从企业角度看，任何试图破坏信息及信息系统完整性、机密性的网络活动都被视为入侵行为。入侵检测技术广泛应用于云系统中，以减轻内部攻击、泛洪攻击、端口扫描、虚拟机攻击和hypervisor攻击等入侵行为。

在边缘计算中，外部和内部攻击者可以随时攻击任何实体。若没有实施适当的入侵检测机制来发现终端设备和边缘节点的恶意行为或协议违规，则会逐步破坏服务设施，进而影响整个网络。

但是，在万物互联环境下，由于设备结构、协议、服务提供商的不同，难以检测内部和外部攻击[9]。此外，如何通过资源能力受限的边缘设备间的系统来进行全局的入侵检测，使其能够在大规模、广泛地理分布和高度移动的环境中得到应用，具有十分重要的意义。

3.4 隐私保护

万物互联系统的目标是通过收集海量数据为用户提供多种个性化服务。由于终端设备资源受限，缺乏对数据加密或解密的能力，这使得它容易受到攻击者的攻击。

边缘计算将计算迁移到临近用户的一端，直接对数据进行本地处理、决策，在一定程度上避免了数据在网络中长距离的传播，降低了隐私泄露的风险。然而，由于边缘设备获取的用户第一手数据，能够获

得大量的敏感隐私数据。如何能够保证用户在使用服务的同时又不泄露其敏感信息对边缘计算中的隐私保护算法提出了更高的要求。

3.5 密钥管理

密钥管理包括从密钥产生到密钥销毁的各个方面，主要表现于管理体制、管理协议和密钥的产生、分配、更换和注入等，包含密钥生成、密钥分发、验证密钥、更新密钥、密钥存储、备份密钥、密钥的有效期、销毁密钥这一系列的流程。密钥在已授权的加密模块中生成，高质量的密钥对于安全是至关重要的，整个密码系统的安全性并不取决于密码算法的机密性，而是取决于密钥的机密性。一旦密钥遭受泄露、窃取、破坏，机密信息对于攻击者来说已经失去保密性。由此可见，密钥管理对于设计和实施密码系统而言至关重要。

在万物互联环境中，由于云服务商、边缘服务商和用户对密钥管理系统与信息技术(IT)基础设施具有不同的所有权和控制权，这使得面向边缘计算环境的密钥管理比传统信息系统的密钥管理更为复杂。因为每个应用出于特定的安全目的管理其安全密钥，使得跨应用密钥管理变得尤为复杂，参与多个应用程序的用户设备需要管理多个安全密钥或口令，增加了密钥泄露的风险并危及服务的安全性。显然，在大规模、异构、动态的边缘网络中，保证用户和用户之间、用户和边缘设备之间、边缘设备和边缘设备之间、边缘设备和云服务器之间的信息交互安全，给边缘计算模式下实现高效的密钥管理方案带来了严峻的挑战。

4 结束语

随着万物互联时代的到来，基于云计算模型的集中式大数据处理模式已经无法满足网络边缘设备所产生海量数据处理的实时性、安全性和低能耗等需求。为此，将原有云计算中心的部分或者全部计算任务迁移到数据源的附近执行，边缘计算在梯联网、工业机器人、无人驾驶、智慧交通等领域扮演着越来越重要的角色。作为一种新型的去中心化架构，它将云计算的存储、计算和网络资源扩展到网络边缘，以支持大规模的协同万物互联应用。然而，由于边缘设备更加靠近网络边缘侧，网络环境更加复杂，并且边缘设备对于终端具有较高的控制权限，导致其在提高万物互联网络中数据传输和处理效率的同时，不可避免地带来一些新的安全威胁，如物理安全、网络安全、数据安全、应用安全等。同时，边缘计算模式也给身份认证、访问控制、入侵检测、隐私保护、密钥管理等方面带来了严峻的挑战。为此，我们需要清晰地认识边缘计算安全框架和业务流程，设计安全的边缘计算架构，这些对于促进边缘计算的进一步普及和发展具有十分重要的意义。

参考文献

[1] 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. DOI:10.7544/issn1000–1239.2017.20160941
[2] 施巍松, 刘芳, 孙辉, 等. 边缘计算[M]. 北京：科学出版社. 2018
[3] 边缘计算产业联盟, 工业互联网产业联盟. 边缘计算与云计算系统白皮书[R]. 2018
[4] HE D J, CHAN S, GUIZANI M. Security in the Internet of Things Supported by Mobile Edge Computing [J]. IEEE Communications Magazine, 2018, 56(8): 56–61. DOI:10.1109/mcom.2018.1701132
[5] KOSCHER K, CZESKIS A, ROESNER F, et al. Experimental Security Analysis of a Modern Automobile[C]//2010 IEEE Symposium on Security and Privacy. USA: IEEE, 2010: 447–462. DOI:10.1109/SP.2010.34
[6] 云计算白皮书[EB/OL]. [2018–12–20]. http://www.199it.com/archives/764250.html
[7] 卿昱. 云计算安全技术[M]. 北京: 国防工业出版社, 2016:53–54
[8] HE D B, ZEADALLY S, WU L B, et al. Analysis of Handover Authentication Protocols for Mobile Wireless Networks Using Identity–Based Public Key Cryptography [J]. Computer Networks, 2017, 128: 154–163. DOI:10.1016/j.comnet.2016.12.013
[9] PRABAVATHY S, SUNDARAKANTHAM K, SHALINIE S M. Design of Cognitive Fog Computing for Intrusion Detection in Internet of Things[J]. Journal of Communications and Networks, 2018, 20(3): 291–298. DOI:10.1109/jcn.2018.000041

作 者 简 介

马立川，西安电子科技大学网络与信息安全学院师资博士后；主要研究方向为隐私保护、边缘计算安全等。

裴庆祺，西安电子科技大学教授、博士生导师、综合业务网理论与关键技术国家重点实验室(ISN)成员、区块链应用与评测研究中心主任，西安市移动边缘计算及安全重点实验室主任，陕西省区块链与安全计算重点实验室执行主任；主要研究方向为认知网络与数据安全、区块链、边缘计算及安全等领域。

肖慧子，西安电子科技大学通信工程学院在读博士研究生；主要研究方向为边缘计算和物联网中的安全与隐私问题。