



专题：智能边缘计算

面向智慧医疗的可信边缘计算

彭绍亮, 白亮, 王力, 程敏霞, 王树林

(湖南大学信息科学与工程学院, 湖南 长沙 410082)

摘要: 随着物联网技术的飞速发展, 为了更好地发展现代医学, 避免信息“孤岛化”危机, 满足边缘设备所产生的海量数据在时效性与计算性能等方面的要求, 将边缘计算与智慧医疗结合是时代的新趋势。但是, 边缘计算具有一定的开放性, 容易存在安全隐患, 所以面向智慧医疗的边缘计算体系的安全与隐私保护问题越来越受到人们的重视。通过介绍面向智慧医疗的边缘计算体系及其架构, 阐述了边缘计算中智慧医疗所遭遇的安全隐患, 并介绍了部分学者针对安全隐患提出的解决方案, 最后总结了安全防护框架及探讨该框架下安全与隐私保护的具体方案, 为智慧医疗边缘计算的可信研究提供一定的帮助。

关键词: 物联网; 边缘计算; 智慧医疗; 隐私保护

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020174

Trusted edge computing for smart healthcare

PENG Shaoliang, BAI Liang, WANG Li, CHENG Minxia, WANG Shulin

College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

Abstract: With the rapid development of internet of things technology, in order to better develop modern medicine, avoid the “isolated” crisis of information, and meet the requirements of timeliness and computing performance of massive data generated by edge devices, it is a new trend of the times to combine edge computing with smart healthcare treatment. However, edge computing has a certain degree of openness, and it is prone to potential safety hazards. Therefore, people pay more and more attention to the security and privacy protection of edge computing system for smart healthcare treatment. The edge computing system and its architecture for smart healthcare were introduced, and the security risks encountered by smart healthcare in edge computing was explained, and some scholars’ solutions to the security risks were introduced. Finally, a security framework, and specific solutions for security and privacy protection under the framework were put forward, which providing some help for the trusted research of smart healthcare edge computing.

Key words: internet of things, edge computing, smart healthcare, privacy protection

收稿日期: 2020-04-30; 修回日期: 2020-05-28

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB0202602, No.2018YFC0910405, No.2017YFC1311003, No.2016YFC1302500, No.2016YFB0200400, No.2017YFB0202104); 国家自然科学基金资助项目 (No.U19A2067, No.61772543, No.U1435222, No.61625202, No.61272056)

Foundation Items: The National Key Research and Development Program of China (No.2017YFB0202602, No.2018YFC0910405, No.2017YFC1311003, No.2016YFC1302500, No.2016YFB0200400, No.2017YFB0202104), The National Natural Science Foundation of China (No.U19A2067, No.61772543, No.U1435222, No.61625202, No.61272056)

1 引言

随着万物互联的趋势不断加深,助力智慧医疗^[1]从临床业务信息化走向个性化医疗。智慧医疗是一个以患者为中心的信息体系,利用先进的信息化技术可以改善疾病预防、诊断和研究,并最终让医疗生态圈的各个组成部分受益^[2]。随着医疗数据的不断积累和数据库的不断壮大,医疗信息的数字化采集、处理、存储、传输、决策等端设备的数量不断增加,使数据的增长速度远远超过了网络带宽的增速。国际数据公司(IDC)的报告指出,到2018年年底,有50%的物联网网络面临网络带宽的限制^[3]。同时,思科的报告也指出,物联网设备还将飞速增长,2020年预计有500亿的设备接入互联网,并产生600 ZB的数据^[4],复杂的网络环境对传输和计算时延提出了更高的要求。IDC的报告^[3]也预测到2020年将有超过40%的数据需要在网络边缘侧分析、处理与存储,边缘计算市场预计超万亿美元。所以,将物联网与云计算集成变得越来越重要^[5-8]。

移动设备利用云服务将会导致时延和与流动性相关的问题^[9-10],因此,将边缘计算^[11]与智慧医疗结合是一种新时代新医疗的新趋势^[12],其中,常见的3种边缘计算模型是:Cloudlets^[13]、雾计算(fog computing)^[14]和移动边缘计算(mobile edge computing, MEC)^[15]。但是,边缘计算的内容感知、实时计算、并行处理等开放特性,使在云计算环境下就已经存在的数据安全与隐私问题变得更加突出^[16]。根据福布斯2015年发布的报告^[17],预计基于云的安全支出将增加42%;根据另一项研究,到2015年,IT安全支出已增加到79.1%,每年增长超过10%。IDC在2011年表明,74.6%的企业客户将安全性列为主要挑战。同时,智慧医疗存在着数据质量较低、敏感数据外泄以及外部恶意窃取等信息安全风险^[18]。迄今为止,面向智

慧医疗的可信边缘计算还没有一个统一的安全防护标准。因此,研究如何构建一个有效的信息安全策略和安全运营体系,对于边缘计算下的智慧医疗的发展已经刻不容缓。

2 面向智慧医疗的边缘计算体系

边缘计算具有去中心化、数据本地化和低时延等特点^[19-20],将智慧医疗与边缘计算的结合具有重大意义。一方面可以提供更高效、便捷的医疗服务,简化医疗流程;另一方面可以提供更公平、开放的医疗资源供给,在数字化基础上的信息化技术又将医学数字信息的“孤岛”状态打破,形成彼此联系。

常见的面向智慧医疗的边缘计算体系架构如图1所示。

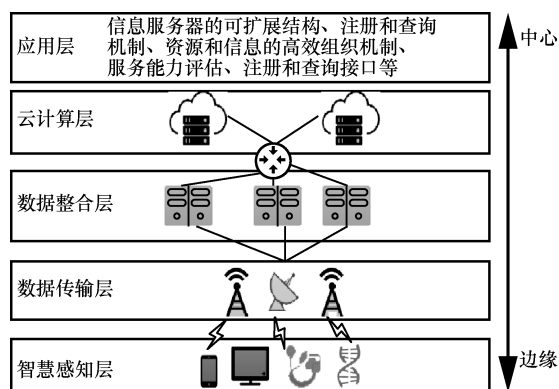


图1 面向智慧医疗的边缘计算体系架构

- 智慧感知层由医疗感知设备、数据采集设备组成,负责医疗数据的感知采集。
- 数据传输层通过移动通信网、互联网和无线网状网(wireless mesh network, WMN)等将智慧感知层采集的数据进行传输。
- 数据整合层通过感知、关联、溯源等手段建立集成创新体系和示范动态数据中心,根据数据的不同类别完成经验模型库和循证模型库的建立。经验模型指的是一些不能通过理化设备检测所能得到的一些关键症状,如既往病史、家族病史、职业、外部



气温、季节等，还包括一些偶发指标，如午后低烧、晨起咳嗽、月经不调、胸闷，气短、发声改变、小腹坠胀，头晕眼花等。循症模型指的是通过理化设备（如可穿戴设备，无创血常规、无创血糖仪、B超、CT等）检测所能得到的一些关键症状，如血压、血糖、心率、心跳、脉搏、白细胞、红细胞、巨噬细胞、血小板、血沉等。

- 云计算层将数据传输层传输的整合数据通过密集型计算，处理成医生所需的信息的功能。例如，神经元算法、人工智能^[21]、机器学习、大数据处理、症状树、算法集成平台等，用来处理用户数据。
- 应用层是结合医疗行业的某些需求，实现智能化的一个过程，主要用来解决的是信息处理和人机交互等问题，比如，手机客户端：针对线上用户，设计了疾病筛查入口，针对自身的疾病，病人如果有初步认识，就可以通过疾病筛查的方式，进一步了解该疾病的可能性。线下网点：由于疾病的复杂性，很多情况下单凭症状很难精准定位疾病本身，同时，由于线上用户专业医疗知识的缺乏，很难准确描述自身的实际症状，因此，设计了线下网点就诊功能。患者可以在有医疗背景的操作人员辅助下，完成症状的人机交互。还能有效地提升患者就诊体验，减少患者排队等候时间。患者在挂号结束后，通过CDSS的诊断建议，做相应的理化指标检查，患者可以拿着理化指标检查数据完成医生诊断、处方，节省患者1/3的就诊时间，降低医生30%的工作量。

由此可见，智慧医疗边缘计算为全球医疗水平的全面提升带来助力，同时，也为不同地区的患者带来更加安全、及时、有效的医疗救助。下面介绍几个将智慧医疗与边缘计算结合比较优秀的案例。

Muhammad等^[22]提出了一种使用深度学习，边缘计算和云计算的新型智能病理检测系统。传感器将捕获人的脑电图（EEG）信号，并将该信号发送到附近的边缘计算服务器。服务器会将预处理步骤分配给可用的边缘设备。然后，预处理后的信号将被发送到云计算服务器。在云服务器中，建议的基于树的深度模型将从EEG信号中提取深度特征。信号属于正常人还是病理人的分类决策将分配给利益相关者。Li^[23]提出了一种边缘学习即服务（EdgeLaaS）框架，以本地处理健康监管数据。在这种框架下，边缘学习节点可以在发生某些紧急情况时实时帮助患者从正确的监护人那里选择更好的建议。其框架有两个应用案例：快速自助；移动帮助预呼叫。Tuli^[24]提出了一个名为HealthFog的新颖框架，用于将深度学习集成到Edge计算设备中，并将其部署到心脏病自动分析的实际应用中。HealthFog使用IoT设备将医疗作为雾服务提供，并根据用户的要求有效地管理心脏病患者的数据。支持雾的云框架FogBus用于在功耗、网络带宽、时延、抖动、准确性和执行时间等方面部署和测试所提出模型的性能。HealthFog可配置为各种操作模式，这些模式可根据需要在不同的雾计算方案中以及针对不同的用户要求，提供最佳的服务质量或预测准确性。Ray等^[25]提出了一种用于电子医疗的基于边缘IoT的新型架构，即EH-IoT，并开发了一个演示测试平台，可以最大程度地减少对物联网云分析或存储设施的依赖性。

智慧医疗的边缘计算体系虽然给全球互联带来了很大的收益，从面向智慧医疗的边缘计算体系架构中可以看到，边缘计算相较于云计算虽然存在其优势，但是边缘计算一样存在着安全隐患。

3 面向智慧医疗的边缘计算体系的安全与隐私保护的问题

智慧医疗与边缘计算的结合作为一种新兴的

医疗模式,在一定程度上实现了医疗信息的共享,成为医疗改革的助推器,为各地区的患者提供等额的医疗资助以及更精确的医疗服务。但是,作为新兴的医疗模式,边缘计算的开放性、多样的数据类型、海量的数据规模等都给智慧医疗的边缘计算体系带来了数据安全、隐私安全等问题。隐私安全的问题来源于物联网的发展、患者权益维护意识、数据增值等方面,如图2所示。

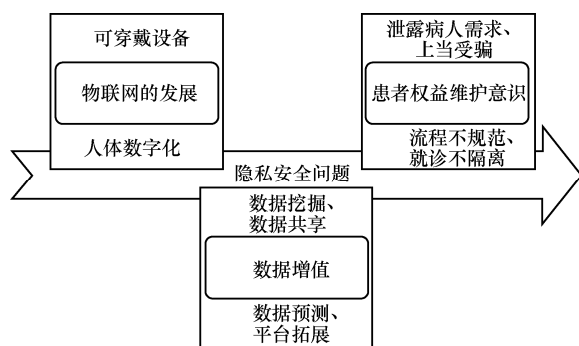


图2 隐私安全问题的来源

(1) 物联网的发展

随着物联网技术的快速发展,患者的医疗数据逐渐走向数字化,可穿戴设备的出现^[26]标志着用户的数据将有设备不打扰人们生活的情况下直接采集,虽然提供了便利,用户可以足不出户就能上报身体数据。但是,Paul等^[27]指出应明确移动医疗可穿戴设备的数据所有权问题,保证在采集大量用户数据的前提下兼顾其安全与隐私。数据在采集以及传输过程中可能受到攻击,用户的安全与隐私受到威胁。

(2) 数据的增值

随着智慧医疗平台的推广,医疗数据的共享范围也逐渐变大,患者的医疗数据不再局限于某个医院内部,更有甚者是一个地区、一个城市乃至一个国家的共享,患者的医疗数据的价值得到成倍的增值,这使得患者数据在大部分不知情的情况下被商业化^[28],这对用户的安全和隐私构成了极大的威胁。

(3) 患者权益维护意识

随着医疗数据的共享,大部分用户的数据在其不知情的情况下被医院共享出来,例如,随着智慧医疗的发展,基因技术也逐渐成熟,作为观测样本的患者在不知情的情况下其DNA样本数据被研究人员作为科研成果公布出来,更有甚者被用来作为信息交易的筹码^[29],所以说在没有一个规范的数据分享流程时分享患者的医疗数据是一件危险的事情。

4 面向智慧医疗的边缘计算体系的安全与隐私保护的核心框架

为了更好地保护医疗数据的隐私与安全,很多专家学者进行了研究。Pasupuleti等^[30]提出了一种针对移动设备的外包云数据隐私保护方案,该方案采用概率公钥加密技术和关键字排名搜索算法,在资源受限的移动终端上实现隐私保护的排名查询。首先,移动用户生成文件索引,并对数据和索引进行加密上传。其次,为了访问云中存储的密文数据,用户为关键字生成陷门并发送到云端。最终,云服务器根据搜索陷门向用户返回基于相关性得分的排序匹配数据,进而解密得到原始数据。Bahrami等^[31]在移动多云计算环境下提出了一种轻量级加密方法来存储云上的数据。该方法采用基于混沌系统的伪随机置换来实现轻量级加密,其置换操作是在移动设备上进行的,而不是在云端,从而保护数据隐私。Li等^[32]提出了一种隐私保护的数据利用系统,通过引入私有云代理作为数据所有者/用户和公共云之间的访问接口,实现了精确的隐私保护关键字搜索和细粒度的访问控制。随着基于位置服务的普及,位置隐私问题也成了广为关注的研究点。Chen等^[33]提出了一种基于分布式缓存推送的位置隐私保护方案。该方案引入了一种分布式缓存代理,用于将经常访问的位置相关数据存储缓存在缓存代理中,并且将位置数据推送给移动用户。如果用户的位置



数据在缓存数组中，则用户不会与基于位置的服务器进行通信，进而不会暴露自己的真实位置，实现位置隐私保护。Wei 等^[34]在移动在线社交网络环境下设计了一种位置隐私保护共享系统 MobiShare。该系统能够实现可信与不可信用户之间的位置共享，并支持范围查询和用户定义的访问控制。在共享过程中通过将用户身份和匿名位置信息分别存储在两个实体中，即使其中一个实体受到攻击，用户的位置隐私也能得到保护。

从上述参考文献中，可以得出保护用户隐私的核心在数据安全、隐私保护、身份认证、访问控制 4 个方面，其保护用户隐私的核心框架如图 3 所示。

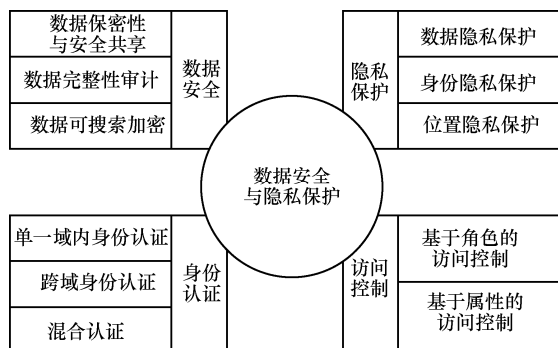


图3 隐私安全保护研究的核心框架

- 数据安全，即保证用户的数据具有保密性，实现安全共享而不暴露用户的隐私信息。其中，通过数据审计确保数据传输的完整性，通过数据的可搜索加密技术利用云端、边缘端服务器庞大的计算资源来实现密文上的关键字查找。
- 隐私保护，保证用户的数据、位置和身份信息是保密的，不可以被攻击者挖掘的数据。例如，通过 RSA 加密算法加密用户的隐私信息，并以假名的方式进行数据交互等。
- 身份认证，即在不泄露用户隐私信息的前提下进行用户身份的匿名认证。其中，有单一域内认证、跨域身份认证和混合认证 3 种

模式；对用户身份进行认证的认证方法有智能卡身份认证、公私钥对加密认证、零知识证明、生物认证等。

- 访问控制，即对用户身份的属性与角色权限访问不同的数据，确保用户数据不被攻击者恶意提取，造成不必要的损失。

5 面向智慧医疗的边缘计算体系的安全与隐私保护方案

为了更好地保护面向智慧医疗的边缘计算体系中用户数据的隐私与安全，本文采用以下 4 个方面来保护用户数据安全。

(1) 多维约束下的隐私度量

从参考文献[35]所提出的匿名认证方案中，可以知道将患者身份信息匿名的根本目标是要让攻击者无法将用户信息（感知数据和指令信息等）与信息的所有者联系起来。因此，衡量算法隐私保护强度最直观的度量指标是信息被识别率（identified rate, IR）。被识别率一般可以通过统计得到，但对某特定时刻匿名区域中的请求 q 。需要不经过统计而直接给出一个隐私度量 $g(q)$ ，使得 $g(q)$ 值较大的一组请求相应的信息被识别率较小（统计意义上的）。不难发现，可用的隐私度量不止一个，本文认为好的隐私度量应该满足下面的关系，即：如果对于 $g(q)$ 值为 g_0 的请求集合 $Q = \{q | g(q) = g_0\}$ ，存在一个理论上的轨迹被识别率下限 $IR_{\min}(g_0)$ ，那么，实际的信息被识别率 $IR_{\min}(q)$ 与 $IR_{\min}(g_0)$ 越接近越好。

基本想法是，对于用户 u_i 的一个给定服务请求， q 假设经过 k 匿名保护之后，产生了 q 的信息匿名集 $U = \{u_1, \dots, u_k\}$ ，若用户 u_i 发送 q 的概率为 $p(u_i \xrightarrow{cm} q)$ ，则根据香农公式可知，信息“请求 q 的发送者”的熵为 $H(q) = -\sum_{u_i \in U} p(u_i \xrightarrow{cm} q) \log p(u_i \xrightarrow{cm} q)$ 。利用指数函数的单调性，可定义隐私度量 $PD(q) = 2^{H(q)}$ 。可以看到

$PD(q)$ 越大, $H(q)$ 也越大, 那么隐私保护的强度也就越高。

在得到隐私度量后, 对于复杂环境下信息隐私泄露风险的评估, 可通过对现有各种信息匿名方法进行多种富异构信息去匿名化攻击, 或是有针对性地设计新的基于边缘计算的攻击方式, 得到不同信息匿名方法在面对不同攻击时的隐私度量, 进而给出统计意义上的隐私泄露风险量化指标。

(2) 云边端协同的数据访问控制及安全共享机制

面向不同服务功能的需求, 对数据进行分类操作, 结合函数加密(如基于属性的加密)方法, 协同终端设备和边缘设备的计算存储资源, 为数据的分享及使用制定细粒度的访问控制方案。首先, 对用户终端产生的数据进行分类, 比如用户个人信息 M_0 以及针对不同服务功能的数据 $(M_0, \dots, M_n)$, 按照不同的安全需求进行安全级别的划分。一般来说, 用户的个人信息只有为用户提供个性化服务的时候才会需要被服务提供者访问, 但是服务信息能为全局的资源分析提供基础。因此, 用户的个人信息相比服务信息需要更强的保护方案。为了实现细粒度的访问控制, 用户可以将个性化的信息存储在本地终端, 将服务信息提交给边缘服务器和云服务器分析和管理。而且, 也可以针对不同功能的数据实行更加细粒度的管理。

(3) 云边端协同的网络化服务安全验证机制

针对边缘服务端及其服务的安全验证问题, 可以构建一个安全验证体系。该验证体系一方面可以考虑采用基于区块链^[36]的远程证明衡量边缘服务器平台的安全; 另一方面, 采用基于区块链的服务安全性验证, 通过白名单、数字证书和完整性度量帮助终端检查边缘服务端所提供的服务的安全性, 最终确保终端可从安全的边缘服务端获取安全的服务。

(4) 数据隐私保护的增量匿名设计及质量评估

当数据和指令信息等发生微量变化时, 针对边缘计算低时延的需求, 增量匿名算法对动态信息进行匿名增量处理。假设用户有以前的版本 $T_1, \dots, T_{p-1}$, 现在需要处理 T_p , 其中 T_i 是 T_{i-1} 数据变化后的更新版本, 并且假设数据是“垂直”更新的, 即数据表的准标识符是固定的, 而记录是随时间动态增加的。本文将在此增量发布模型中研究记录插入、删除和修改的情况下, 感知信息隐私泄露的威胁模型, 然后对这 3 种操作的增量更新算法分别进行研究; 对插入操作, 先根据插入元组与标识符 QI 组的语义贴近度确定要插入的 QI 组, 再将其转化成泛化元组。对删除操作, 根据元组与泛化元组的映射关系确定待删除元组在 k 匿名数据集中的位置, 再进行删除; 对修改操作, 则分解为删除和插入两步操作来完成。此外, 对数据质量提出更加合理的度量标准, 拟采用多维空间覆盖区域的大小度量匿名后数据集的失真程度, 评估隐私保护方案的有效性。

6 结束语

在全球互联、万物互联的时代背景下, 智慧医疗是实现医疗信息化的最终目标, 同时, 考虑云计算的弊端, 已逐渐不能满足智慧医疗对大数据的处理、信息交互的时效性。所以将智慧医疗与边缘计算相结合是时代背景下的要求。本文介绍了智慧医疗结合边缘计算的相关技术以及其面临的安全和隐私问题, 同时, 针对这个问题参考部分已提出的解决方案提出自己的隐私安全保护框架和部分解决方案, 安全运营是智慧医疗得以在边缘计算体系下成长的重要保障。因此, 确保面向智慧医疗边缘计算体系的隐私与安全是让医疗信息化走向智能的助推器。

参考文献:

- [1] GONG Y G, XIN C. Healthcare information integration and



- shared platform based on service-oriented architectures[C]//Proceedings of 2010 2nd International Conference on Signal Processing Systems. [S.l.:s.n.], 2010.
- [2] 糜泽花, 钱爱兵. 智慧医疗发展现状及趋势研究文献综述[J]. 中国全科医学, 2019, 22(3): 366-370.
- MI Z H, QIAN A B. Research status and trend of smart healthcare: a literature review[J]. Chinese General Practice, 2019, 22(3): 366-370.
- [3] TURNER V, GANTZ J F, REINSEL D, et al. The digital universe of opportunities: rich data and the increasing value of the internet of things[J]. IDC Analyze the Future, 2014(16): 13-19.
- [4] Cisco. Cisco global cloud index: forecast and methodology[Z]. 2015.
- [5] LEE H. Framework and development of fault detection classification using IoT device and cloud environment[J]. Journal of Manufacturing Systems, 2017(43): 257-270.
- [6] STERGIOU C, PSANNIS K E, KIM B G, et al. Secure integration of IoT and cloud computing[J]. Future Generation Computer Systems, 2018(78): 964-975.
- [7] VERMA P, SOOD S K. Cloud-centric IoT based disease diagnosis healthcare framework[J]. Journal of Parallel and Distributed Computing, 2018(116): 27-38.
- [8] HSU T C, YANG H, CHUNG Y C, et al. A creative IoT agriculture platform for cloud fog computing[J]. Sustainable Computing: Informatics and Systems, 2018(10): 285.
- [9] AHMED E, AKHUNZADA A, WHAIDUZZAMAN M, et al. Network-centric performance analysis of runtime application migration in mobile cloud computing[J]. Simulation Modelling Practice and Theory, 2015(50): 42-56.
- [10] PACE P, ALOI G, GRAVINA R, et al. An edge-based architecture to support efficient applications for healthcare industry 4.0[J]. IEEE Transactions on Industrial Informatics, 2018, 15(1): 481-489.
- [11] SHI W, SUN H, CAO J, et al. Edge computing-an emerging computing model for the Internet of everything era[J]. Journal of Computer Research and Development, 2017, 54(5): 907-924.
- [12] 盛煜, 彭恒, 冯毅. 基于 5G 移动网络的智慧医疗应用[J]. 邮电设计技术, 2019(7): 3-7.
- SHENG Y, PENG H, FENG Y. Intelligent medical application based on 5G mobile network[J]. Designing Techniques of Posts and Telecommunications, 2019(7): 3-7.
- [13] YAQOOB I, AHMED E, GANI A, et al. Mobile Ad Hoc cloud: a survey[J]. Wireless Communications and Mobile Computing, 2016, 16(16): 2572-2589.
- [14] BAO W, YUAN D, YANG Z, et al. Follow me fog: toward seamless handover timing schemes in a fog computing environment[J]. IEEE Communications Magazine, 2017, 55(11): 72-78.
- [15] AHMED E, REHMANI M H. Mobile edge computing: opportunities, solutions, and challenges[J]. Future Generation Computer Systems, 2017: 59-63.
- [16] 何晓琳. 健康医疗可穿戴设备数据安全与隐私研究进展[J]. 中华医学图书情报杂志, 2016, 25(10): 32-37.
- HE X L. Advances in data security and privacy protection of wearable health and medical devices[J]. Chinese Journal of Medical Library and Information Science, 2016, 25(10): 32-37.
- [17] RAMACHANDRA G, IFTIKHAR M, KHAN F A. A comprehensive survey on security in cloud computing[J]. Procedia Computer Science, 2017(110): 465-472.
- [18] 徐玲玲, 徐婷婷. “互联网+”背景下智慧医疗应用现状研究[J]. 智能计算机与应用, 2020(1): 44-49.
- XU L L, XU T T. The research on the current situation of intelligent medical application under the background of big data[J]. Intelligent Computer and Applications, 2020(1): 44-49.
- [19] ZHOU Y, TIAN L, LIU L. Fog computing enabled future mobile communication networks: a convergence of communication and computing[J]. IEEE Communications Magazine, 2019, 57(5): 20-27.
- [20] QI Y, TIAN L, ZHOU Y. Mobile edge computing-assisted admission control in vehicular networks: the convergence of communication and computation[J]. IEEE Vehicular Technology Magazine, 2018, 14(1): 37-44.
- [21] 王志宏, 杨震. 人工智能技术的哲学及系统性思[J]. 电信科学, 2018, 34(4): 12-21.
- WANG Z H, YANG Z. Philosophy and systematic thinking of artificial intelligence technology[J]. Telecommunications Science, 2018, 34(4): 12-21.
- [22] MUHAMMAD G, ALHAMID M F, LONG X. Computing and processing on the edge: smart pathology detection for connected healthcare[J]. IEEE Network, 2019, 33(6): 44-49.
- [23] LI G L. EdgeLaaS: edge learning as a service for knowledge-centric connected healthcare[J]. IEEE Network, 2019, 33(6): 37-43.
- [24] TULI S. HealthFog: an ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments[J]. Future Generation Computer Systems, 2020(104): 187-200.
- [25] RAY P P, DASH D, DE D. Edge computing for internet of things: a survey, e-healthcare case study and future direction[J]. Journal of Network and Computer Applications, 2019(140): 1-22.
- [26] CYR B. Security analysis of wearable fitness devices (fitbit)[J]. Massachusetts Institute of Technology, 2014: 1-14.
- [27] PAUL G, JAMES I. Privacy implications of wearable health devices[C]//Proceedings of the 7th International Conference on Security of Information and Networks. New York: ACM Press, 2014.
- [28] 洪海林. 个人信息的民法保护研究[M]. 北京: 法律出版社,

2010.

HONG H L. The research on the protection of personal information in civil law[M]. Beijing: Law Press China, 2010.

- [29] 王强芬. 大数据时代背景下医疗隐私保护的伦理困境及实现途径[J]. 中国医学伦理学, 2016(4): 685-689.

WANG Q F. Ethics predicament and protection path of medical privacy in the era of big data[J]. Chinese Medical Ethics, 2016(4): 685-689.

- [30] PASUPULETI S K, RAMALINGAM S, BUYYA R. An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing[J]. Journal of Network and Computer Applications, 2016(64): 12-22.

- [31] BAHRAMI M, SINGHAL M. A light-weight permutation based method for data privacy in mobile cloud computing[C]//Proceedings of 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. Piscataway: IEEE Press, 2015: 189-198.

- [32] LI J W, LI J, CHEN X F. Privacy-preserving data utilization in hybrid clouds[J]. Future Generation Computer Systems, 2014(30): 98-106.

- [33] CHEN M, LI W, LI Z, et al. Preserving location privacy based on distributed cache pushing[C]//Proceedings of 2014 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2014: 3456-3461.

- [34] WEI W, XU F, LI Q. Mobishare: flexible privacy-preserving location sharing in mobile online social networks[C]// Proceedings of International Conference on Computer Communications. [S.l.:s.n.], 2012: 2616-2620.

- [35] ARFAOUI A, KRIBECHE A, SENOUCI S. Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications[J]. Computer Networks, 2019(159): 23-36.

- [36] 张云勇, 程刚, 安岗. 区块链在电信运营商的应用[J]. 电信科学, 2020, 36(5): 1-7.

ZHANG Y Y, CHENG G, AN G. Application of blockchain in telecom operators[J]. Telecommunications Science, 2020, 36(5): 1-7.

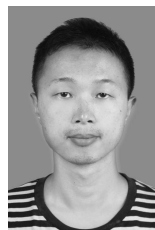
[作者简介]



彭绍亮 (1979-), 男, 湖南大学信息科学与工程学院教授、博士生导师, 湖南大学教育舆情研究中心副主任, 国家超级计算长沙中心副主任, 湖南省“杰出青年”, 湖南大学“岳麓学者”, 主要研究方向为高性能计算、大数据、生物信息、人工智能、区块链等。



白亮 (1992-), 男, 湖南大学信息科学与工程学院博士生, 主要研究方向为生物信息学、边缘计算、区块链技术等。



王力 (1989-), 男, 湖南大学信息科学与工程学院硕士生, 主要研究方向为生物信息学、智慧医疗、药靶预测等。



程敏霞 (1995-), 女, 湖南大学信息科学与工程学院硕士生, 主要研究方向为生物信息学、机器学习、智慧医疗等。

王树林 (1966-), 男, 博士, 湖南大学信息科学与工程学院教授、博士生导师, 主要研究方向为生物信息学、软件工程和人工智能。