

智慧健康研究综述：从云端到边缘的系统

邱宇¹ 王持¹ 齐开悦² 沈耀¹ 李超¹ 张成密³ 过敏意¹

¹(上海交通大学大学计算机科学与工程系 上海 200240)

²(上海交通大学电子信息和电气工程学院 上海 200240)

³(上海交通大学医学院附属新华医院 上海 200092)

(ed3rss@sjtu.edu.cn)

A Survey of Smart Health: System Design from the Cloud to the Edge

Qiu Yu¹, Wang Chi¹, Qi Kaiyue², Shen Yao¹, Li Chao¹, Zhang Chengmi³, and Guo Minyi¹

¹(Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240)

²(School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240)

³(Xinhua Hospital Affiliated to Shanghai Jiao Tong University School of Medicine, Shanghai 200092)

Abstract Smart health is a real-time, intelligent, ubiquitous healthcare service based on the IoT aware network and sensing infrastructure. Thanks to the rapid development of related technologies such as cloud computing, fog computing and IoT, research on smart health is gradually on the right track. This paper analyzes research on smart health in recent years and then discusses the development of smart health from both cloud and edge, including cloud computing, fog computing, IoT sensors, blockchain, and privacy and security. At present, in the research of cloud and smart health, the focus is on how to use the cloud to complete the challenges of massive health data and improve service performance, including related issues such as storage, retrieval and calculation of health big data in the cloud. At the edge, research focuses on the collection, transmission, and computation of health data, including sensors and wearable devices for collecting health data, various sensor networks, and how to process health data and improve service performance at the edge. As an emerging technology, blockchain has a wide range of applications in smart health. We discuss typical smart health application, blockchain in smart health and privacy and security issues related to smart health. Finally, we present challenges and opportunities for smart health in the edge computing era.

Key words smart health; cloud computing; fog computing; sensor; blockchain; privacy and security; survey

摘 要 智慧健康是基于物联网的环境感知网络和传感基础设施的实时的、智能的、无处不在的医疗保健服务。得益于云计算、雾计算以及物联网等相关技术的快速发展,关于智慧健康的相关研究也逐渐步入正轨。近年来对于智慧健康的相关研究,主要从云端和边缘这2个主要方向展开,其中包含了云、雾计算,物联网传感器,区块链以及隐私和安全等相关技术。目前,在云和智慧健康的研究中,关注点在于如何利用云去完成海量健康数据的挑战和提升服务性能,具体包括健康大数据在云中的存储、检索和计算等相关问题。而在边缘,研究重点转变为健康数据的采集、传输和计算,具体包括用于采集健康数据的各类传感器和可穿戴设备、各类无线传感器技术以及如何边缘处理健康数据并提升服务性能等。最后,

收稿日期:2019-01-04;修回日期:2019-06-27

基金项目:上海交大-卫宁健康联合实验室项目(2017001);上海交通大学医工交叉项目(YG2016QN73)

This work was supported by the Project of SJTU-Winning Joint Laboratory (2017001) and the SJTU Medical-Engineering Cross Project (YG2016QN73).

通信作者:齐开悦(tommy-qi@sjtu.edu.cn)

对典型的智慧健康应用案例、区块链在智慧健康中的应用以及相关隐私和安全问题进行了讨论,并提出了智慧健康服务在未来的挑战和机遇.

关键词 智慧健康;云计算;雾计算;传感器;区块链;隐私和安全;综述

中图法分类号 TP391

随着人口老龄化加速,慢性病的流行以及流行病的爆发,越来越多的关注点聚焦到居民生活质量和健康问题上,人们越发重视健康问题.然而,人口平均年龄的增长和慢性病的流行导致人们对医疗资源需求的快速增长,特别是在人口集中度较高的城市地区,各级医院和诊所的医疗资源十分宝贵,难以对病人提供实时的医疗保障.可以设想,在不久的将来,医疗健康服务将从医院提供的集中式医疗服务逐渐转变为普遍存在和实时运作的智慧健康服务.这种演变有3个导因:首先,人们对更全面、更智能和更主动的医疗健康服务的需求不断增长,其中服务的关键部分是通过实时的、不引人注意的健康监测来提供可用于智慧健康服务的个人健康数据;其次,智慧健康服务的基础设施通用和共享的特性将会减轻现阶段不断增加的医疗健康服务费用;最后,随着云计算、雾计算和物联网传感器等相关技术的快速发展,给医疗服务形式的转变奠定了坚实的基础.

这种医疗服务形式的转变逐渐催生了智慧健康的概念,概括来说,智慧健康是利用物联网的环境感知网络和传感基础设施来提供实时的、智能的和无处不在的医疗保健服务.智慧健康服务首先需要是实时的,例如对于一些关键生理指数的监测是不接受较大延迟的,以避免延误时机,这种实时性需要通过云计算、雾计算和边缘设备的配合来达成.其次智慧健康服务是智能的,利用在雾端的一些智能程序或者边缘的智能传感器等,智慧健康服务可以提供更智能的医疗服务.最后智慧健康服务是无处不在的,无论人身在何处,利用周围的物联网传感器以及可穿戴传感器设备,可以实现无处不在的智慧健康服务.

如图1所示,如今智慧健康服务对性能、能效、安全和隐私保护的需求导致系统必须在云、终端设备以及二者之间架设多样化的计算层,通过跨层次的设计和管理提供优质的智慧健康服务.可以看到,当终端传感器收集到相关人体生理指数后,对于数据的处理通常存在多种选择.对于实时性和移动计算要求不高的海量数据处理,可以通过云端代理

(cloud proxy)直接把数据上传到云中;对于实时性和移动计算要求高的智慧健康服务则通过雾端代理(fog proxy)把数据先上传到雾计算层(如智能网关),在雾计算层中,雾会根据当前的负载情况、云端运行情况以及任务属性来合理地决定如何处理数据.图1描述了3种上传策略(upload scheduler):云端计算、云雾端协助计算和雾端计算.

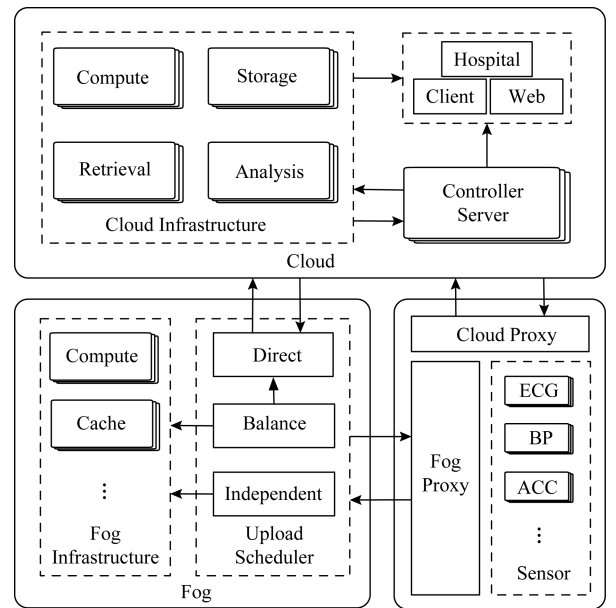


Fig. 1 Cloud-edge cross-layer design of smart health
图1 智慧健康的雾云端跨层设计

接下来,本文将会从云端到边缘来详细讨论智慧健康的相关研究与发展并列典型的智慧健康应用,并且,由于区块链在智慧健康领域有广泛的应用场景,还会对区块链在智慧健康中的应用进行讨论,最后会讨论智慧健康的隐私和安全以及未来会遇到的一些机遇和挑战.

1 云端的智慧健康

得益于物联网和移动网络的快速发展,越来越多的研究关注到智慧健康以及各类生物传感器等相关的便携式医疗设备^[1].这些医疗设备可以收集各种各样的实时健康数据,例如血压、体温和心率等,

这些健康数据具有非常大的量级,并且很难在便携设备中进行存储、分析和处理.如何快速有效地处理健康大数据成为了一项挑战.大数据通常是指 EB 以及更大范围数据量的数据,它具有大容量、多样化、快速、复杂等特点^[2].健康大数据不仅具有大数据的所有特点,而且健康大数据对于人的价值和意义也是其他大数据所不具备的.对于智慧健康大数据,通常的单机系统和便携移动设备没有足够的能力去存储和处理,而云计算平台具有强大的计算存储能力,目前,在云端存储、分析和处理健康大数据是最合适且最具性价比的方法.

云计算是一种计算资源的抽象,它把动态可扩展且被虚拟化的计算资源作为服务提供给使用者,具有按需提供服务、广泛访问方式、聚集的资源池和快速弹性分配等基本特点^[3-6].正是得益于云计算的这些基本特点,智慧健康服务提供者可以在基于云的系统框架上搭建出实时的、智能的和无处不在的智慧健康应用,并且可以满足智慧健康中大数据的要求.可以说,云计算的高速发展为智慧健康服务的

实际落地打下了坚实的基础.基于此,越来越多的研究开始关注到云计算和智慧健康服务,如何利用云计算来实现实时的智慧健康服务以及如何满足健康大数据的要求成为了研究的重点.本文归纳、分析和总结了近年来关于云和智慧健康的相关研究,接下来将会从智慧健康大数据的存储、检索和数据处理 3 个方面来介绍智慧健康大数据在云端的研究和发展.

1.1 健康大数据在云端的存储

随着医疗信息化的不断发展以及各类医疗传感器技术的快速发展,实时产生的健康大数据越来越多,在单机系统或便携移动设备中存储数据变得越来越困难^[7].并且,大多数传感器健康数据都是实时生成的,特别是一些由可穿戴设备产生的健康监测数据,必须及时地上传和处理,以免错过最佳时机.如表 1 所示,对于健康大数据在云端的存储,根据研究侧重点的不同,本文将从 3 个方面来讨论:面向异构数据的存储、高可靠性和高容错性的存储、基于隐私和安全的存储.

Table 1 Storage System of Smart Health in Cloud

表 1 智慧健康大数据的云端存储系统

References	Focus	Data	Technology	Advantage
Ref[8]	Data Complexity Optimization	Health Data	NoSQL	Overcome Pattern Differences
Ref[9]	Data Complexity Optimization	Health Data	SQL/NoSQL	Data for Different Structures
Ref[10]	Reliability, Fault Tolerance	Image and EHR	HDFS	High Fault Tolerance
Ref[11]	Reliability, Fault Tolerance	Hospital File	DFS	Mass Storage
Ref[12]	Privacy and Security	EHR	RAID-3	Data Security
Ref[13]	Privacy and Security	Health Data	Encryption	Personal Privacy

1.1.1 面向数据复杂性优化的存储

与传统的互联网大数据不同,各类医疗健康设备会产生大量复杂的异构健康数据,这些结构各异的医疗健康数据很难用一种统一的模式去规范和定义,传统的关系型数据库将很难满足医疗健康数据异构性和复杂性的存储要求^[14].如何存储健康大数据成为了智慧健康研究的一项关键挑战.目前,得益于非关系型数据库的出现和快速发展,商业和开源解决方法都开始利用非关系型数据库来代替传统的关系型数据库去处理健康大数据.与传统的关系型数据库系统相比,非关系型数据库打破了模式字段的限制,提供了无模式的数据存储,更加灵活.一些常见的非关系型数据库如表 2 所示:键值数据库、文档数据库、列数据库、图形数据库和时间序列数据库.

Table 2 NoSQL Databases in Medical Health

表 2 非关系型数据库在医疗健康中的应用场景

Database	Type	Application
Redis	Key-Value	Health Data Cache
Memcached	Key-Value	Health Data Cache
MongoDB	Document	Heterogeneous Health Data
CouchDB	Document	Heterogeneous Health Data
HBase	Column	Massive Health Data
Neo4J	Graph	Medical Information Search
InfluxDB	Time Series	Electronic Health Record

由于非关系型数据库不需要固定的表格模式,对于异构健康大数据的存储,采用非关系型数据库是一种常见的做法.Lin 等人^[8]提出了一种基于非关系型数据库的快速处理、存储、检索和分析医疗健康

大数据的综合方法.该方法基于非关系型数据库,使用以患者为中心的数据架构,以实现数据的快速存储和灵活扩展,其中的时间序列模式可以用于生成患者记录的可视化表示,可以作为医生给患者提供咨询的参考.Lin 等人提出的方法可以克服各类医疗健康大数据的模式差异,并且确保了灵活性和大规模存储.

医疗健康大数据一般来自多个不同的源,例如各类功能形式各异的医疗传感器、大型医疗设备和便携医疗设备等,这些数据形式和结构都不相同,因此数据库必须采用一系列不同的模型来存储和处理不同形式的医疗健康大数据.Kaur 等人^[9]提出了一个管理健康大数据的框架,该框架结合了关系型数据库和非关系型数据库(图形和文档数据库),以适应云中各种不同形式的医疗健康大数据.综上所述,基于非关系型数据库的智慧健康服务可以有效地应对异构健康大数据的存储问题.

1.1.2 高可靠性和高容错性的存储

由于健康大数据的特殊性,健康大数据不仅数据量十分巨大,同时也要求非常高的安全性,对于数据丢失的情况是零容忍的.为此,在为医疗健康大数据设计存储和文件管理系统方面展开了一系列工作,文件和存储系统不仅要满足存储海量的医疗健康数据的需求,同时需要保障高可靠性和高容错能力,以提供可靠的医疗信息服务.分布式文件系统是由大量存储节点通过网络连接在一起的大型文件系统,可以存储海量的数据,并且数据通常会通过保持副本等的方法来保障服务的高可靠性^[15].目前,许多研究采用了分布式文件系统来解决海量医疗健康数据的存储问题,并保障医疗服务的高可靠性和高容错性.

HDFS (Hadoop distributed file system) 是 Hadoop 的一个分布式文件系统,可以存储海量大数据.Yang 等人^[10]试图解决在云端存储共享医学图像和电子病历的问题,开发了一种基于 HDFS 的医学成像文件系统 (medical image file accessing system, MIFAS),该系统是一个带有分布式文件系统的医学成像系统,可以实现高可靠性的医疗数据存储,并具有高容错性.

Guo 等人^[11]提出了一个基于云计算的智能医院档案管理系统,旨在改善传统医院管理系统的一些局限性.这些限制包括一些单机硬件设备的存储容量限制以及跨不同平台的资源共享导致的硬件性能降低.Guo 等人提出的分布式文件系统由主服务

器和多个服务器块组成.大文件被分成固定大小的块,每个块存在 3 个备份块.主服务器管理文件系统元数据,包括命名空间、访问控制、文件块映射和相关信息的物理地址.该模型采用大量低成本服务器集群,可灵活地允许应用程序克服物理边界,根据需求最大限度地利用系统资源.

1.1.3 基于隐私和安全保护的存储

与传统的互联网大数据相比较,医疗健康大数据的隐私和安全显得更为重要,个人隐私是一个十分敏感的话题.如果只是简单把医疗健康数据存储在云端,可能会导致很多隐私和安全问题.特别是随着互联网数据量的迅速增长以及医疗信息化的加速,人们对于隐私和安全的问题越来越看重.如何在云端安全地存储健康大数据成为了一大挑战.

RAID-3 是传统的磁盘存储阵列策略,可保障磁盘数据的安全性.Chen 等人^[12]提出了一种使用 RAID-3 算法存储分布在 2 个不同云和本地站点的电子病历的新方法.通过 RAID-3 算法,存储在每个云中的分段数据毫无意义,不能单独使用.该方法将患者的数据存储在云中,以满足 EHR 存储空间不断增长的需求,同时也满足数据隐私和安全的需求.

Fan 等人^[13]开发了数据捕获和自动识别 (data capture and auto identification reference, DACAR) 平台,以解决各种医疗健康服务的安全性、完整性、保密性和集成问题.DACAR 平台利用私有云进行数据存储,使用混合云进行托管服务.该平台采用了数据库级加密、数字签名验证、散列和完整性校验等技术,以保障医疗健康数据的安全性和个人隐私.

1.2 健康大数据在云端的检索

存储在云端的医疗健康数据来自于各类医疗设备、医学传感器以及异构嵌入式设备等,这些海量数据往往具有不同的模式和结构.对这些形态各异的存储在云端的医疗健康大数据的高效检索变成了一件极具挑战性的事情.Natarajan 等人^[16]通过从基于电子健康记录搜索系统的历史检索记录中分析了医疗信息检索系统需要具有的功能以及需要满足哪些特定的需求.Yang 等人^[17]分析了医疗搜索引擎的查询日志记录,旨在促进电子健康记录中的信息检索效率,分析结果表明,医学领域的信息需求比通用网络搜索引擎的信息需求要复杂得多.查询准确性和时间效率是评估医疗检索系统性能的 2 个重要指标.

1.2.1 医学信息检索

在云端进行大规模医学信息的检索是一件非常耗时的操作,并且由于医学信息的隐私性,大多在云

端的医学信息都是加密过的,这更加大了检索的难度.如何有效地提升医学信息的检索效率成为了研究重点.Mu 等人^[18]在实验中检验了查询复杂性以及查询扩展策略对基因组信息检索的影响.他们发现采用查询扩展策略并没有真正地提高效率.结果还表明字符串索引扩展比单词索引扩展更有效,具有较少数量术语的查询优于具有较多术语数的查询.基于这些发现,Mu 等人建议基因组信息检索系统应支持灵活的查询扩展策略,以适应具有不同复杂程度的查询.

加密文档上的数据检索是云存储中非常重要的技术,其中敏感医学数据的加密是在将文档存储到云之前的必要操作.许多现有的可搜索加密方案都集中在单用户场景上.Yang^[19]关注了多发送方和多用户的应用场景,提供了灵活的加密文档搜索方案.该方案中,基于属性的加密技术(attribute based encryption, ABE)用于支持细粒度访问控制,并且启用同义词关键字搜索.张丽丽等人^[20]提出了一种对于加密电子医疗记录的检索方案,该方案利用分层属性矢量表示方法实现了灵活而复杂的多域关键词连接查询,例如子集查询和范围查询等.

1.2.2 医学图像检索

医学图像的检索和信息查询不同,信息查询只需要匹配相似关键字或字符串,找到相关内容即可,但这对于医学图像检索是存在问题的,医学图像检索目标是帮助相关医疗人员做出决策.在这些场景中,给定所需要检索的医学图像,目标是从云端数据库中检索出相似的图像或者相关的医学信息,所查询到的内容可以帮助相关医疗人员了解所查询图像的参考医学解释.如果检索系统给出的图像或者信息与所查询图像的语义不符合,这将会导致使用人员的不信任.另一方面,如果检索系统给出的结果与所查询医学图像相似,但却是错误的结果,那么这将导致相关医疗人员的误判.

Yang 等人^[21]提出了一个医学图像检索的增强框架,旨在保持图像视觉和语义相似性.他们设计了一种增强算法来有效地学习距离函数,可以保持检索结果和图像的语义相似性,且具有很低的计算成本.Rahman 等人^[22]提出了一种基于内容的图像检索框架,适用于不同成像模态的医学图像.Rahman 等人所提出的框架包括用于图像预滤波的机器学习方法、使用统计距离测量的相似性匹配以及相关反馈方案.该图像检索框架可以有效地缩小语义差距并提高检索效率.

医学信息检索和图像检索是健康数据在云端检索的两大重要方向,除了研究如何在云端检索数据,还需要关注如何去整合检索各种分布式和异构的医疗信息系统.Cabarcos 等人^[23]描述了一个检索框架,它从各种分布式和异构的来源检索生物医学信息,对其进行管理以改善所获得的结果并缩短响应时间,最后将其整合以使其对相关医疗人员有用,提供有关患者的所有可用信息.Kim 等人^[24]提出了一个客户端-服务器代理框架,允许门户通过内联网和因特网访问不同的医院信息系统.Kim 等人提出的代理能够远程访问医院通常封闭的信息系统和服务器,该服务器索引所有医疗数据,并且允许进行复杂的数据检索.

1.3 健康大数据在云端的计算

医疗传感器和便携移动设备具有有限的计算能力,不允许现场实时处理医疗健康数据,所收集到的数据需要传送到计算能力更强大的节点进行处理.云计算平台是一个拥有强大计算能力的平台,并且随时随地可供访问,能够帮助边缘医疗设备和便携移动设备计算和处理数据.利用云计算不仅可以在云中做医疗健康大数据处理,还帮助缓解边缘医疗设备的负载压力,显著提高移动设备在医疗保健中的使用效率.

1.3.1 在云端做医疗大数据处理

云计算平台的规模非常大,大型商用云计算平台甚至拥有上万台服务器来提供服务,得益于云计算的强大计算能力,可以在云端对各类医疗大数据进行分析和处理,这类任务通常需要强大的计算能力,而不要求实时性.

生物信号分析是一件耗时耗力的事情,通常需要云计算的支持.Shen 等人^[25]提出了一种生物信号分析的云计算架构(bio-signal analyzing cloud computing architecture, BACCA).该系统基于面向服务架构的概念,在云中集成了异构平台、协议和应用程序.在该生物信号分析框架中,对于不同的数据集,脑电波生物信号分析的总体准确度已提高到接近 98%.

在云中对海量医疗大数据使用数据挖掘发现深层次信息是一种常见做法.Takeuchi 等人^[26]开发了一个基于云的个人医疗保健系统.该系统通过便携移动设备把个人健康数据按照时间序列存储在云中.当数据足够时,在云中使用数据挖掘方法自动提取有用的健康信息,例如隐藏在大数据中的个人健康信息.

由于电子健康记录的异构特性和庞大的规模,在云中对电子健康记录分析和处理已经成为常态.在过去几年中,贝叶斯网络、神经网络、模式识别和逻辑回归等方法常常被用于从电子健康病历中提取患者信息和预测相关疾病.Kurt 等人^[27]把 3 种不同的分类方法在预测冠状动脉疾病方面的表现进行了比较,结果发现,基于多层感知器的神经网络方法在预测中表现出最佳性能.综上所述,通过把健康大数据迁移到云数据中心中处理,可以帮助智慧健康应用挖掘出更多的隐藏在健康数据中的深层次医疗信息.

1.3.2 利用云缓解边缘医疗设备压力

边缘设备往往不具备充足的计算能力,这限制了移动医疗服务的性能和效率.同时由于移动医疗服务要求很高的实时性,若把所有数据全部放在云端处理,会因为网络传输导致较大的延迟.如何去结合边缘医疗设备和云计算来提供高效实时的移动医疗服务成为了一项挑战.

利用云帮助边缘设备缓解部分高性能计算的压力是一种可以有效提高服务性能的方法.Nkosi 等人^[28]提出了一种云计算框架,用于减轻移动设备在提供移动健康服务时执行多媒体算法和安全算法的压力.该框架表明,多媒体和安全算法相关操作可以在云计算平台中执行,允许移动医疗服务提供商扩展其移动健康应用程序的功能,超出现有移动设备的限制.

云和边缘设备的协同工作可以有效提升移动医疗服务质量.Wang 等人^[29]提出了一种新的混合移动云计算解决方案,以实现更有效的个性化医疗监控.他们对基于移动云的心电图监测分析的案例进行了研究,并开发了移动云原型.该混合移动云解决方案可以在诊断准确性、执行效率和能源效率方面显著强于传统的基于移动的医疗监测,并具有解决个性化医疗保健中大规模数据分析的潜力.

受限于边缘医疗设备的性能,通过边缘设备提供快速准确的医疗诊断比较困难,云计算可以帮助智慧健康应用达到这一要求.Hsieh 等人^[30]基于云计算构建了 12 导联心电图服务,以实现无处不在的 12 导联心电图远程诊断.该服务利用云计算来加强边缘医疗设备的能力,大大提高医疗服务质量和效率.

2 边缘的智慧健康

目前,在云端智慧健康的研究中,主要是针对健康大数据的存储、分析和计算等.云与智慧健康的结

合可以帮助智慧健康服务解决大数据和性能的问题.通过云的辅助,智慧健康服务可以存储和处理海量健康大数据,并从大数据中挖掘出有用的信息.但是光有云是不够的,如引言所述,智慧健康服务是实时的、智能的以及无处不在的.为了满足智慧健康服务的实时、智能和无处不在的要求,需要在网络边缘做非常多的工作.本文总结、分析和归纳了近年来的相关研究,把智慧健康在边缘的研究分为了健康数据的采集、计算和无线传输技术 3 个主要方面.

2.1 智慧健康数据的采集

智慧健康大数据经历了一个快速增长的过程,而其中大量健康数据来自不引人注意的传感器和可穿戴设备.传感器和可穿戴技术被视为智慧健康的基石,是整个智慧健康系统的数据来源.微小的传感器可以编织或集成到服装、配件和生活环境中任何不起眼的角落,从而可以在日常生活中连续实时地获取医疗健康信息.传感器甚至可以设计为粘贴电子纹身并直接印在人体皮肤上,以实现长期健康监测.与个人健康息息相关的生理信息包括心率、呼吸频率、血压、血氧饱和度和肌肉活动等,从生理信息中提取的数据可以提供健康状况指标,具有巨大的诊断价值.

2.1.1 传感器技术

传感器是整个智慧健康体系的基石,是监测系统的基本元素,需要长期准备并实时地测量相关的生理指数.微型生物传感设备、智能技术、微电子和无线通信等相关技术的发展使得各类传感器能够更有效、更快地感知和测量数据,同时具有更低的能耗和更少的处理资源.如表 3 所示,列举了常见的监测各类生理指数的传感器技术.

体温(body temperature, BT)是可穿戴传感器测量的用于人类活动监测的常见生理参数之一.皮肤上测量的温度变化可以指示人体体温发生了什么,可以用来检测可能导致各种健康状况的医学症状,包括中风、休克和心脏病等.在智慧健康服务中,除了用体温来确定病人的生理状况这类最常见的应用外,还可以用于确定人的活动状态^[31],甚至一些可穿戴设备可以从人体体表散发的余热中收集能量^[32]等.温度传感器在人类生活中非常普遍,常见的测量温度的传感器方法有水银、红外线、热敏电阻和热电偶等.

血压(blood pressure, BP)是体检中最常测量的参数之一.血压可以判断心脏功能与外周血管阻力,同时也是诊断疾病、观察病情变化与判断治疗效

果的一项重要内容.脉搏波传播方法^[33]是一种用于血压测量的有前景的技术.它是基于脉搏波速度与动脉压之间的关系来测量血压,该测量方法不需要血压计袖带来辅助测量.

Table 3 Sensor Technology of Bio-Signal
表 3 主要生理指数的边缘传感器技术

Bio-Signal	Method	Type of Sensor	Size of Sensor	Skin Contact
Body Temperature	Mercury, Infrared Ray, Thermistance	Skin Patch, Probe	Tiny	NA
Blood Pressure	Pulse Wave Propagation Method	Arm Cuff-based Monitor	Medium	Direct
Heart Rate	Photoplethysmography	Skin Electrodes	Tiny	Direct/Indirect
Electrocardiography	Capacitance-coupled Sensing Method	Skin Electrodes	Tiny	Indirect
Accelerometer	Piezoelectric, Piezoresistive, Capacitance	Accelerometer	Tiny	No
Respiratory Rate	Piezoelectric Cable Sensor, Impedance Plethysmography	Piezoelectric Sensor	Small	No

心率(heart rate, HR)是最常见的受监测的生理参数之一,它在人类的健康和疾病监测中起着关键作用,用于心率监测的传感器方法也非常多.光电容积描记术^[34](photoplethysmography, PPG)是被广泛地用于监测心率,它利用光电传感器检测经过人体血液和组织吸收后的反射光强度的不同,描记出血管容积在心动周期内的变化,从得到的脉搏波形中计算心率.PPG 传感器可以集成到日常生活配件中(如手表、耳环和手套),以实现不显眼的测量.Baek 等人^[35]提出了一种用于 PPG 测量的间接接触传感器,采用控制电路调节适应各种类型衣物的光强度.另一方面,Poh 等人^[36]表明可以使用数码相机从受试者脸部远程捕获的 PPG 中测得心率和呼吸率.

心电图(electrocardiography, ECG)可以提供关于心跳速率和规律性等生理信息,在心脏疾病的诊断中经常使用.基于此,可穿戴式心电图传感器可以用于心血管疾病的短期评估,特别是对于患有慢性心脏病的人.电容耦合传感方法是一种测量生物点位的传感器方法,可以用于测量心电图和脑电图^[37]等,对于这种方法,皮肤和电极形成 2 层电容器.在没有与身体直接接触的情况下,可以避免粘合剂电极在长期监测中引起的一些问题,例如皮肤感染和信号劣化.

呼吸率(respiratory rate, RR)是监测病人健康状况的重要生理参数,呼吸是人体内外环境之间进行气体交换的必需过程,人体通过呼吸过程来吸入氧气和呼出二氧化碳,从而维持正常的生理功能.压电传感器,其传感元件是压电聚合物,可以被用于呼吸率监测^[38].阻抗体积描记法是另一种广泛使用的呼吸测量方法^[39].位于肋骨和腹部的 2 个正弦线圈

由产生高频正弦电流的电流源驱动.呼吸期间胸部的运动引起线圈电感的变化,从而调制正弦电流的幅度,从中可以解调呼吸信号.

加速度计(accelerometer, ACC)是一种监测人类活动的传感器,它主要用于测量沿特定轴的特定频率范围的加速度.它们可以用于许多目的,例如跌倒检测^[40]和运动分析^[41]等.对于加速度的测量,有基于压电、压阻或可变电容等几种方法可用.通常它们都采用相同的操作原理,通过使弹簧或类似等效部件与测量的加速度成比例地拉伸或压缩来测量加速度.

2.1.2 智能可穿戴设备

智慧健康系统通常将传感器技术与物联网集成,使医疗保健系统能够监控患者.目前,在工业界中已经有非常多的智能可穿戴设备,这些设备可以帮助监测生理参数.通常,智能可穿戴设备具有这些特点:小型化、低能耗、智能化和个性化.

FuelBand 是一款可以戴在手腕上的活动追踪器.FuelBand 可以跟踪一段时间内所进行的运动和消耗的卡路里,并把腕带的读数分享到在线社区.Apple Watch 作为一款智能手表,它不仅支持记步、监测睡眠和记录能量消耗等,还支持监测心率和绘制心电图等专业医疗数据.Fitbit 手环不仅可以记录步伐和计算活动消耗,还可以智能地判断是否在运动以及何项运动等.随着相关技术和算法的不断发展 and 突破,例如更加精确的新型记步算法^[42],这些智能可穿戴设备变得越来越重要,成为了智慧健康系统中重要的一环,作为智慧健康系统中数据来源的关键组件,它们承接了大量健康数据采集的工作,为后端系统提供了丰富的、多种多样的健康数据,利用这些数据可以对人体健康状况进行详细的分析.

2.2 智慧健康数据在边缘的计算

在云计算平台存储、检索和处理医疗健康数据是一种非常高效的可以帮助智慧健康应用快速落地并发挥作用的架构。云可以帮助智慧健康服务应对大数据和性能的挑战,但却很难满足智慧健康实时性的要求。得益于物联网和传感器技术的发展,越来越多的医疗健康数据在网络边缘产生。大量的医疗健康数据需要实时处理,并且这类医疗健康数据是难以容忍网络延迟和卡顿的,对于实时性的要求非常高,这对于云计算平台的压力非常大。因此现在有很多研究没有把对于医疗健康数据的计算和处理放在云计算中心,而是迁移到更靠近边缘节点的雾计算平台,通过雾计算平台来有效提高服务的实时性,满足智慧健康服务高实时性的需求。

2.2.1 雾计算和智慧健康

思科率先提出雾计算的概念,是云计算概念的一种延伸^[43],雾计算把服务和计算移动到更加贴近用户端的位置,满足低延时、实时性的应用,同时可以减轻网络的负担。雾计算是指靠近边缘的微型云计算结构,不同于传统的云计算结构,雾计算中的数据和应用程序的资源被放置在边缘节点和云之间的逻辑位置,也被称为雾网络。Li 等人^[44]对边缘计算环境中的系统架构和资源管理给出了全面介绍,但并没有针对智慧健康应用进行专门介绍。

在智慧健康服务的发展中,越来越多的健康数据在边缘节点产生,例如利用医疗传感器监控病人生理指数等。由于边缘设备功率和性能受限,对采集的健康数据很难做到实时处理,而如果将这些数据全部传输到云计算中心处理又会导致较大延迟,影响用户体验。并且,物联网的大规模实施预计将引入数十亿连接到互联网的边缘设备,鉴于连接设备数量众多以及数据量较大,与云连接也会出现大量延迟的情况。基于此,雾计算成为了智慧健康应用的一个中间处理站。将这类健康数据从大规模数据中心迁移到靠近边缘节点的微型数据中心,不仅可以降低延迟、提高边缘设备的效率,同时也降低了大量的数据请求对后端云计算平台施加的网络压力^[45]。例如,一些小型嵌入式医疗设备的数据处理,不需要将每条数据都传入到云计算中心进行处理,而是将一些实时性要求高的任务交给智能网关处理,这将节省大量的网络成本和提高实时性。综上所述,在云和边缘节点之间架设雾计算层,可以有效提高服务实时性,雾计算是向分层系统架构和更快响应的设计转变的重要范例。

2.2.2 利用雾来提高智慧健康服务

物联网和传感器技术的不断发展使我们能够开发出更智能的医疗保健解决方案,不仅适用于医院内部,还可以应用在日常生活中,保障医疗健康。在大多数基于物联网的医疗保健系统中,尤其是在智慧家居和智慧医院中,在传感器基础设施网络和后端互联网之间需要桥接点,即通常所说的网关。网络边缘的网关通常只执行基本功能,例如在互联网和传感器网络中使用的协议之间进行转换和传输实时数据。这些网关对传感器网络和传输的数据进行有效的控制。利用这些网关在网络边缘的战略地位,可以提供更多的服务,如本地存储和本地实时数据处理,从而呈现出智能电子健康网关。通过这类智能电子健康网关,可以在传感器节点和云计算平台之间形成地理分布的中间智能计算层来实现智慧健康物联网系统中的雾计算概念。通过智能电子健康网关来负责处理传感器网络和远程云计算中心的一些负担,雾计算架构可以应对无处不在的医疗保健系统中的许多挑战,例如移动性、能效和可扩展性等。

物联网技术可以应用于智慧健康等相关领域,作为无线传感器网络与传统互联网之间的桥接,物联网网关在智慧健康应用中发挥着重要作用。Zhu 等人^[46]根据典型的物联网应用场景和电信运营商的要求,提出了基于 ZigBee 和分组协议的物联网网关系统,介绍了无线传感器网络与移动通信网络之间的数据传输、不同传感器网络协议的转换和无线传感器网络的控制功能,设计了原型系统并进行了系统验证。

Emara 等人^[47]提出了一个基于智能网关的通用框架,用于无线传感器网络和互联网互连。该框架允许访问各个传感器节点,并为以数据为中心的传感器网络启用基于互联网的查询功能。它还提供一个网络到另一个网络的透明访问,而无需修改在任一网络中运行的协议。此外,该框架可以扩展为多网关架构从而提供容错和负载平衡能力。

Mueller 等人^[48]展示了一个通用的传感器网络平台 SwissGate,它为传感器网络编程提供了高级接口,并提供了一个多层架构,可以有效地处理和优化传感器网络的运行。

Bimschas 等人^[49]提出了智能网关中间件的设计,它允许通过为传感器网络和互联网提供简化的接口在网关上执行应用程序代码。由于网关完全了解并控制传感器网络和互联网,因此智能网关可以充当性能增强代理和智能缓存,以保护传感器网络的有限资源。

Shang 等人^[50]提出了一种新颖的可配置智能物联网网关,它具有 3 个重要的优点:首先,网关具有插入式架构,其具有不同通信协议的模块可以根据不同的网络进行定制;其次,它具有统一的外部接口,适合灵活的软件开发;最后,它具有灵活的协议,可将不同的传感器数据转换为统一格式.与同类研究相比,网关具有更好的可扩展性、灵活性和更低的成本.

Stantchev 等人^[51]提出智能医疗健康基础设施的 3 层架构,并提供了一个示例用例作为基于智能传感器的医疗基础设施的模板.该架构基于面向服务的体系结构,架构集成了角色模型、分层云计算架构以及雾计算通知范例,以便为医疗健康应用提供可行的中间计算层架构.

Cloudlet 是位于蜂窝网络边缘的具有较强移动性的微型数据中心,它是一种云计算中心的扩展,把云计算资源迁移到蜂窝网络的边缘,服务于低延时、实时性的任务.Cloudlet 可以帮助智慧健康应用减少延迟以实现更快的响应,并提高应用交互性.Quwaider 等人^[52]介绍了基于 Cloudlet 的大规模医疗体域网系统.目标是通过使用 Cloudlet 系统来动态选择收集到云的数据,从而最小化端到端的数据包成本,同时还尝试通过动态选择邻居云来最小化端到端的数据包延迟,从而最小化整体延迟,最终实现对于医疗健康数据的实时监控.智慧健康服务还可以利用 Cloudlet 平台来帮助卸载任务,Lo'ai 等人^[53]提出了基于 Cloudlet 的移动医疗模型,模型首先会从 Cloudlet 中寻找服务,只有当 Cloudlet 中没有该服务时,用户才会连接到医疗云.除此之外,Chen 等人^[54]建立了基于 Cloudlet 的新颖的医疗数据共享系统,在减少通信能耗的同时可以防止恶意攻击.EI Amraoui 等人^[55]提出一种基于 Cloudlet 和软件定义网络的新架构,可以平滑设备和访问网络的异构性,并通过云环境实现医疗数据收集和分析的快速访问.总之,作为云和边缘传感器网络的中间层,Cloudlet 可以帮助智慧健康服务减少延迟、辅助计算以及减少能耗.

随着雾计算的研究发展,智慧健康应用从中受益颇多,其中智能网关和微型数据中心可以大幅提高智慧健康应用的实时性,以及为智慧健康应用提供更多辅助功能.

2.3 智慧健康的无线传输技术

在智慧健康系统中,为了实现全面的健康服务,常常会在人体上布置众多的生理传感器,这些传感

器协同工作,实时地、连续不断地采集所需要的生理指数,并发送到中心节点,由中心节点进行数据聚合等处理后再传送到相应的后端系统.为了实现这些生理传感器与中心节点的协同工作,研究人员提出了体域网(body sensor network,BSN)的概念.体域网是附着在人体上的小型网络,由各类小型生理传感器和中心节点组成.通过体域网,各类传感器设备可以将监测数据传输到中心节点进行数据处理,中心节点对各生理数据进行数据过滤、清洗和聚合等操作后,把数据发送到后端系统.

2.3.1 无线通信标准

传感器网络通常分为有线和无线 2 类,对于前者,使用常规网络线缆会导致系统的故障率上升,并且会影响用户的体验和舒适度.因此,在体域网系统中更多采用无线技术.如表 4 所示,有各种各样的无线技术可用于体域网,常见的例如 Bluetooth,WiFi,ZigBee,WiMAX,MICS 等.

Table 4 Communication Protocol for Smart Health

表 4 智慧健康应用主要依赖的通信协议

Protocol	Range/m	Data Rate/Mbps	Frequency/ GHz
Bluetooth	10-100	1-3	2.4-2.48
ZigBee	1 075	0.25	0.868/0.915, 2.4
WiFi	200	54	2.4, 5
WiMAX	15 000	128	2.3-3.5
MICS	2	0.4	0.402-0.405

ZigBee^[56]是一种低速短距离传输的无线网络协议,媒体访问层和物理层采用 IEEE 802.15.4 标准.得益于 ZigBee 协议的超低功耗,ZigBee 协议通常被用于一些低数据传输速率和长电池寿命的智慧健康应用中^[57-58].这些应用对于数据速率的要求较低,并且通常具有几个月甚至几年的电池寿命.

蓝牙(最初为 IEEE 802.15.1)是一种常见的短距离无线通信技术,通常用于移动设备之间交换数据.它是一种低成本的射频标准,工作在 2.4~2.48 GHz 频段^[59].相对于 ZigBee,蓝牙拥有更快的数据传输速率,并且随着低功耗蓝牙的推广,蓝牙在需要高带宽的智慧健康应用得到了越来越多的使用^[60-62].

WiFi 是一项基于 IEEE 802.11 的无线局域网技术,工作在 2.4 GHz 和 5 GHz,是日常生活中最常见的一种无线网络技术之一.而 WiMAX 是一项基于 IEEE 802.16 的高速无线网络标准,主要用于城域网,传输距离可达几十千米.相较于 ZigBee 和蓝牙,

WiFi 具有更高的功耗,并且存在一些隐私保护问题,不太适合移动计算场景.但在室内监控和活动识别的智慧健康场景中,由于如今室内 WiFi 的普遍性, WiFi 正逐渐发展为主要解决方案^[63-64].

MICS(medical implant communications service)是一种超低功耗的专门用于医疗设备和医学试验的通信协议.MICS 使用 402~405 MHz 频段,一般用于传输低速率数据.MICS 一般用于低功耗和低数据传输速率的场景^[65].

2.3.2 体域网技术的发展

体域网技术是智慧健康服务中的物联网开发的核心技术之一,它负责把各类生理传感器串连在一起,形成一个布置人体上的采集、处理和传输生理指数小型网络系统.体域网系统负责智慧健康服务中的数据来源和预处理,它的性能直接影响到智慧健康服务质量.作为一种小型网络系统,体域网对于能耗、安全和隐私的需求非常高,同时也缺乏高级软件抽象支持.基于此,研究人员把关注点放在了安全、能耗、开发框架等方面.

在能耗方面,Cho 等人^[66]提出了一种用于体域网的高能效双频收发器.该收发器提供 30~70 MHz 体通道通信和 402~405 MHz 医疗植入通信服务,可以实现高达 30%的节能效果.Yoo 等人^[67]介绍了一种自配置的可穿戴 BSN 系统,该系统具有高效率

的无线供电传感器,能够以低功耗连续监测身体选定位置的 ECG 和其他生命信号.

在安全方面,Gope 等人^[68]提出了一种使用体域网基于物联网的医疗保健系统,称为 BSN-Care,系统采用了轻量级匿名身份验证协议和加密方案偏移码本来保证用户信息的安全.在体域网中,由于网络的严格资源限制,只能部署轻量级机制以满足安全需求,于是 Bao 等人^[69]从另一个角度出发,提出用人体心跳脉冲间隔信息来生成识别传感器节点的实体标志符,用以保证安全.人体固有的传递信息能力是保护体域网内无线通信的独特且节省资源的方法.

在开发框架方面,Fortino 等人^[70]基于新兴的基于域的编程范例推出了一个用于体域网的开源编程框架 SPINE,旨在支持体域网应用的快速灵活的原型设计和管理.Lo 等人^[71]提出了一种体域网硬件开发平台.凭借其低功耗、灵活和紧凑的设计,为体域网的研究和开发提供了一个多功能的环境.

3 从云到端的智慧健康应用案例

大量研究也关注到智慧健康相关的应用,越来越多的关于智慧健康的研究应用被开发出来,如表 5 所示,接下来将会介绍其中一些应用案例,包括健康监控系统、疾病预测和防范、智能健康硬件等方面.

Table 5 Typical Application for Smart Health
表 5 面向智慧健康的典型系统应用

References	Type	Bio-Signal	Description	Scalability	Mobility
Ref[72]	Health Monitoring	ECG	Cloud-based ECG Monitoring	High Storage Requirement	No
Ref[73]	Health Monitoring	Voice	Voice Pathology Monitoring	Insufficient Real-time	No
Ref[74]	Health Monitoring	HR, BP, BT	Wireless Bio-signal Monitoring	Difficult with High Traffic	No
Ref[75]	Health Monitoring	NA (Health Data)	Wearable Personal Assistant System	High Processing Capacity	Yes
Ref[76]	Disease Prediction	BP	Hypertension, Fall Event Prediction	Insufficient Accuracy	No
Ref[77]	Disease Prediction	ECG	Heart Disease Prediction	High Power Consumption	Yes
Ref[78]	Hardware Design	BP, HR, ECG	Collect Bio-signal	Hardware Scalability	Yes
Ref[79]	Hardware Design	ECG, RR	HR Detection, Motion Detection	High Power Consumption	Yes
Ref[80]	Hardware Design	NA (Health Data)	Wearable Computing System	High Energy Consumption	Yes
Ref[81]	Data Visualization	NA	Data Visualization and Analysis	Lack of Accurate Analysis	No
Ref[82]	Healthcare Platform	NA	Heterogeneous Medical System	Difficult with High Traffic	No

3.1 健康监测系统

健康监控是目前智慧健康中最多的应用之一,通过实时的生理指数监控,可以有效地帮助诊断和提高健康水平.Hossain 等人^[72]介绍了一个智慧健

康的监测框架,其中 ECG 和其他医疗数据由移动设备和传感器收集,并安全地发送到云,以便医疗专业人员无缝访问.同时框架采用了信号增强、水印和其他相关分析方法,可以避免医疗专业人员的身份盗

用和临床错误.Muhammad 等人^[73]使用物联网云对人们进行语音病理监测的可行性并提出了解决方案.更具体地,在监视框架内基于语音信号的频谱表示上的局部二进制模式和用于检测病理的学习机分类器提出语音病理检测系统.所提出的监测框架可以实现高精度的检测,并且易于使用.Lin 等人^[74]开发了一套实时无线生理监测系统,其功能是通过无线通信信道和有线局域网来监测老年患者的生理状态.该系统通过定制的医疗检查模块采集了体温、血压和心率等数据,医护人员可通过计算机实时地监控病人的生理状态并分析患者的生理变化.除此之外,考虑对于病患的实时监测,有研究设计了基于可穿戴个人设备的生理监测系统^[75],可以实现实时地、不间断地生理指数监测.

3.2 疾病预测和防范

疾病预测和防范是一类可以提前帮助发现患者病情的智慧健康应用,不同于传统的医疗服务,疾病预测和防范可以在问题出现前提醒患者以及帮助患者避免问题的发生.Melillo 等人^[76]描述一个平台的设计和初步验证,该平台用于收集和自动分析生物医学信号,用于高血压患者血管事件和跌倒的风险评估.这个基于云计算的移动健康平台设计灵活、可扩展性高,并通过数据挖掘提供主动远程监控.该系统能够预测未来 12 个月内的血管事件,准确率为 84%,监测摔倒事件的准确率为 72%.

集中式医疗服务资源越来越紧张,给患者提供疾病自测的健康服务变得更加重要.Leijdekkers 等人^[77]开发了一种心脏病发作自测应用,该应用程序允许潜在的受害者在没有医学专家干预的情况下快速评估自己是否患有心脏病.该系统基于移动手机和心电图传感器等技术,通过分析采集的心电图记录来分析用户症状并检测是否心脏病,若存在风险会立刻敦促用户呼叫紧急服务.

3.3 智能健康硬件

基于移动和便携的需求,有许多功能新颖的智能健康硬件被开发出来,这些智能健康硬件为智慧健康服务开拓了一条新的发展道路.Pandian 等人^[78]开发了一种智能背心,该背心通过一系列传感器阵列来采集佩戴者的生理指数,并生成佩戴者健康状况的整体情况.该背心监测的生理指数有血压、心率、心电图和体温等.Di Rienzo 等人^[79]开发了一种可清洗的传感背心,用于记录心率和运动信号.该背心由监测心电图和呼吸率的传感器和用于运动检测、信号处理和无线数据传输电子板组成.该传感背

心不仅能够获得质量非常好的数据,还能检测心率失常事件.除了功能性,还需要考虑到智慧健康硬件性能与能耗的折中,Wang 等人^[80]设计了一种用于可穿戴设备的新型跨端分析引擎架构,该架构实现了可穿戴传感器和具有高能效的数据聚合器的通用分类设计,在延长电池寿命的同时也降低了系统延迟.

3.4 其他应用

健康数据可视化和分析也是常见的智慧健康应用,通过对收集来的实时数据的可视化展示和分析,可以帮助医疗人员更为精准地发现其中的问题.Mohammed 等人^[81]为医疗领域构建一个基于安卓平台的移动应用程序,该应用程序使用物联网和云计算的理念.Mohammed 等人构建的应用程序,为最终用户提供了电子心电图和后台健康数据的可视化.收集的数据可以上传到用户的私有云或特定医疗云,程序保存了所有的健康数据记录,并且可以被医疗人员检索以用于医疗分析.

各类异地、异构的医疗健康信息系统造成了医疗信息孤岛的局面.智慧健康管理平台需要整合各个信息孤岛并加之统一管理,以促进信息共享^[83].Sebestyen 等人^[82]提出并验证一个名为 CardioNet 的应用程序,这是一个分布式医疗系统,连接不同的医疗实体和系统,如医院、急诊室和实验室等.该分布式系统是可以通过网络提供不同的服务,如远程监控、在线咨询和医院活动管理等.

关于智慧健康的应用案例十分多样,它们在各方面帮助人们提高健康水平,缓解了现有医疗制度下的资源压力.

4 智慧健康的新机遇-区块链

近年来区块链技术日益受人关注,作为一种新兴技术,区块链分散、透明和安全的特性使其在医疗方面也存在许多应用价值.区块链本质上是一种分布式数据库技术,它通过工作量证明、分布式时间戳协议、最长链算法以及相关加密算法(如 SHA256)等技术来实现分布式共识机制和用户匿名,这也是区块链的两大重要特征^[84].

如图 2 所示,每一个区块包含有版本号、上一区块散列值、Merkle 根节点、时间戳、随机数和交易数据等,其中前 5 项组成了区块头,每一个区块都必须包含前一个区块头的 SHA256 散列值,这保证了文件基本不可能被篡改,如果篡改某区块必须把后续

所有区块的散列值都改掉,并且每个区块都含有创建时的时间戳,这也保证了区块在时间上有序成链.同时,为了实现共识,区块链采用了工作量证明机制,通过区块中的随机数来实现工作量证明.通过以上的协议和算法,区块链实现了一个分散、透明和安全的分布式数据库.

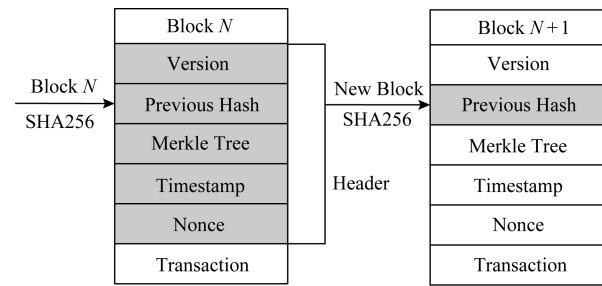


Fig. 2 Data structure of blockchain
图2 区块链数据结构

目前的医疗形式大多是中心化的管理模式,患者的数据都存放在第三方机构中,并且各机构的数据并不互通,形成了一座座信息孤岛.当患者从一家机构换到另一家机构后,之前的所有医疗健康数据都无法共享.这对于患者来说是一种损失,也增加了医疗服务提供者的负担.区块链的去中心化分散管理的特质正好可以解决智慧健康服务的这类需求,它适用于希望彼此协作而不将控制权交给中央管理者的应用.同时,区块链具有的不可篡改和数据加密的特质也可以很好地保证健康数据的正确性以及保护患者的隐私.不仅如此,得益于区块链的分散、透明和安全的特质,智慧健康服务还可以利用区块链促进临床试验正确性保证、解决药品供应链、搭建智慧健康管理平台等.如表6所示,区块链在智慧健康服务中有众多应用,接下来本文将逐一介绍区块链在智慧健康服务中的研究与发展.

Table 6 New Smart Health Service Based on Blockchain
表6 基于区块链的新型智慧健康服务

References	Applications	Platform	Key Technique	Focus	Key Benefit
Ref[85]	Health Data Sharing	Ethereum	Smart Contract	EHR	Decentralized
Ref[86]	Health Data Sharing	Hyperledger Fabric	Channel Formation Scheme	Health Data	Security/Privacy
Ref[87]	Health Data Sharing	NA	Asymmetric Encryption	Medical Image	Security/Privacy
Ref[88]	Clinical Research	Ethereum	Smart Contract	Data Utilization	Transparent
Ref[89]	Clinical Research	NA	Machine Learning	Model Training	Decentralized
Ref[90]	Clinical Research	NA	Timestamp	Clinical Trials	Immutable
Ref[91]	Pharmaceutical Industry	NA	Timestamp	Counterfeit Drug	Transparent/ Immutable
Ref[92]	Pharmaceutical Industry	NA	Smart Contract	Supply Chain	Transparent/ Immutable
Ref[93]	Support Platform	Ethereum	Shared Infrastructure	Management Platform	Decentralized
Ref[94]	Support Platform	NA	Identity Scheme	Management Platform	Decentralized
Ref[95]	Medical Fraud Detection	NA	Proof of Work	Transaction Process	Autonomy

4.1 健康数据共享

通过传感器和可穿戴技术,个人健康数据为医疗健康服务提供了巨大且不断增加的价值,使患者和医疗服务提供者受益,但受制于隐私保护和安全,并不能完全发挥它的价值.个人健康数据通常是极其敏感的个人隐私数据,但不同于常规的个人隐私数据(如家庭地址、信用卡等),健康数据在一定范围内的共享无论对于患者还是医疗服务提供者都有极大的裨益.这类健康数据的共享可以帮助患者、医疗服务提供者以及第三方厂商等获取有用信息,打破信息孤岛,同时,去中心化的健康数据共享也能避免数据被中央管理者控制和篡改.

区块链技术正好符合这类场景的需求,通过区块链可以实现隐私和可访问性的微妙平衡,基于此,许多研究和项目开始侧重于使用区块链来共享健康数据以改善医疗记录管理.Dagher 等人^[85]提出了一个名为 Ancile 的基于区块链的框架,该框架可以实现患者、医疗服务提供者和第三方对于电子健康记录的高效安全的访问以及实现医疗记录的共享,同时可以保护患者敏感信息的隐私.Liang 等人^[86]提出了一种基于区块链的以用户为中心的健康数据共享解决方案,利用区块链渠道机制来保护隐私,并使用区块链的会员管理系统来增强身份管理,最终达到安全共享健康数据的目标.不仅是在医疗记录上,

Patel^[87]开发了一个跨域图像共享框架,该框架使用区块链作为分布式数据库来建立放射学研究的分类帐,同时由患者定义访问权限.该框架被证明可以消除第三方对医学图像访问的安全问题,并且符合可互操作卫生系统的标准,可以很容易地推广到其他医学领域.

4.2 促进医学研究

得益于区块链分散、透明和安全的特点,许多研究开始关注区块链技术在医学研究领域的应用,区块链与医学研究的结合也拓宽了智慧健康服务的应用场景.与传统的中心化管理不同,区块链的去中心化管理令传统医学研究可以以分散合作的形式展开,大幅提高医学数据利用率.并且区块链不可篡改和按时间成链的特性可以提升医学研究数据的可信度,确保数据的可追溯性.区块链作为分布式数据库技术,为医学研究带来了新的活力.

医学研究人员建议使用区块链来促进临床数据的2次使用,Azaria等人^[88]提出了MedRec,一种新颖的分散的记录管理系统,该系统采用区块链技术来处理电子病历和数据.在系统中,医疗利益相关者作为区块链矿工参与网络,他们通过工作量证明协议来维持网络,以换取可访问匿名数据的挖掘奖励.MedRec可以提供大量匿名医疗数据以增强研究人员的能力,同时也可以吸引患者和相关机构发布元数据.除了促进医学临床数据的利用率,区块链技术的出现令分散式的跨机构医学研究得以实现,Kuo等人^[89]描述了一个新的框架ModelChain,使区块链技术适用于医学预测模型的分散研究.不同于传统的集中式架构,每个参与节点都有助于模型参数估计而不揭示任何患者信息,并可以使用来自多个机构的数据进行预测模型学习.在临床试验中,可再现性和正确性是医学研究中的重大挑战,区块链成为了应对这些挑战的关键点,Benchoufi等人^[90]探讨了区块链在临床试验中可以保证整个文档流程的大量历史性数据不可侵犯性,确保数据的可追溯性和防止了后验重建,并允许通过智能合约安全地自动化临床试验.区块链技术确保了临床试验中对于数据安全性的细粒度控制.得益于区块链对于医学研究的促进作用,使得智慧健康服务可以获得更安全、更准确的医学支持.

4.3 改善制药工业安全问题

药品安全问题一直是导致医患关系紧张的重要原因之一,因为药品安全问题而导致的医疗事故频频发生,但是对于非医疗从业人员,很难去分辨药品

的真伪,甚至还为伪造产品花费大量医疗资金.尽管在目前智慧健康服务中,可以从中央管理者获取药品真伪信息,但是确难以避免中央管理者的篡改和欺诈行为.由于伪造药品市场的高额利益和巨大的市场价值,光从管理和法律的角度很难完全消除伪造药品现象.区块链的出现让研究人员看到了从另一个角度去解决这个问题.利用区块链的不可篡改性和完全透明的特点,研究人员试图让药品从原料到生产再到分配这一整个过程都完全曝光在所有人的眼前.

Hyperledger工作组提出了一个使用区块链技术来提高药品供应链安全性的项目^[91],Accenture, Cisco, Intel, IBM, Block Stream, Bloomberg 等公司均参与到此项目中.该项目设想通过使用区块链的时间戳和顺序性,来方便验证药物的生产时间和地点,可以帮助解决伪造药物和不合格药物的问题,确切地说明产品的制造地点.除此之外, Schöner 等人^[92]也提出了一种基于区块链的解决方案,以提高制药行业的供应链安全性.在 Schöner 等人的解决方案中,每个药品附有一个明确的识别标签,允许药品所有权通过区块链上的智能合约验证的可信网络从上游供应商转移到下游消费者.总而言之,区块链作为供应链基础设施可以为全球药物供应链带来完整性、可追溯性和透明性,可以很好地解决伪造药品问题.

4.4 智慧健康支撑平台

目前,大量研究人员关注到区块链与智慧健康的结合,提出了许多创新的研究成果.同时,工业界也不甘示弱,与云、雾跨层设计的智慧健康应用不同,工业界提出了基于区块链的分散管理的、透明安全的智慧健康支撑平台.

Gem Health Network^[93]是一个基于以太坊的区块链网络,通过建立与通用数据基础设施相连的医疗保健生态系统,解决以患者为中心的医疗服务与运营效率之间的权衡,其中包括针对共享数据基础架构的身份方案、数据存储和智能合约应用程序. Gem Health Network 是涵盖整个智慧健康服务的连续统一体,从健康和预防到计费 and 索赔等一系列流程.医疗保健巨头之一飞利浦医疗保健已经宣布加入到 Gem Health Network.

一家位于荷兰的数据安全公司 Guardtime,与爱沙尼亚政府合作创建了一个基于区块链的智慧健康管理平台,可以用来验证患者身份^[94].目前,所有的爱沙尼亚公民、医疗服务提供者都可以使用

Guardtime 平台来获取相关的医疗信息,Guardtime 平台已经运营有超过 100 万的健康记录.

综上所述,区块链在健康数据共享、促进医学研究、规范制药工业和支撑平台等方面具有广泛的应用,并且区块链的影响力还在不断地扩大,相关应用不断崭露头角,例如医学欺诈监测^[95]等.基于区块链的分散管理的智慧健康平台可以帮助运作完整的公共卫生基础设施,并在此之上提供更加完善、安全和智能的服务.

5 智慧健康的隐私和安全

5.1 电子健康记录

个人健康记录(personal health record, PHR)服务允许患者通过网络创建、管理和控制个人健康数据,这使得存储、检索和共享医疗信息更有效率.每个患者可以完全控制个人病历并且可以广泛地与其他用户分享健康数据,包括医疗服务提供者、家庭成员或朋友.由于建设和维护专业化的数据中心所需的成本过高,所以许多 PHR 服务外包给特定的第三方服务提供商.例如 Google Health, Microsoft HealthVault, ICW LifeSensor 等. Li 等人^[96]以及 Löhr 等人^[97]提出了在云中进行 PHR 的信息存储架构的设计方案.

因为其服务中心化的存储方式,PHR 为大多数人都提供了便利的服务,但仍然存在许多安全和隐私风险可能阻碍其广泛使用.如:

1) 患者是否能真正控制他们的敏感个人健康信息(personal health information, PHI)分享,尤其是当这些数据存储在第三方服务器上,而服务提供商可能不是完全可信;

2) 敏感的个人健康记录具有很高的价值,第三方存储服务器通常是各种恶意攻击行为的重要目标,从而可能导致暴露敏感个人健康记录.

因此对于患者来说,足够细粒度的数据访问控制机制是必不可少的.一种可行且有保障的方法是加密外包前的个人健康记录数据.基本上,PHR 所有者自己应该决定如何加密文件并允许哪个集合的用户获取对每个文件的访问权限,只有获得解密密钥的用户才有权访问相应的文件.在必要时,患者也应有撤销相应访问权限的能力^[98].

与由患者管理的 PHR 不同,电子健康记录(electronic health record, EHR)只属于专业健康管理人士管理.在大多数国家,根据法律,PHR 和 EHR 有明确的界限,且要求不同.因此,涉及 EHR 的基础设施通常比简单的基于 PHR 的云模型完全不同.

EHR 模型的基本要求仍然是功能性的存储和在 EHR 中的基本数据操作.EHR 是由医疗保健提供者创建、维护和管理,并可以共享(通过中央云中的 EHR 服务器)给其他专业健康人员.但是 EHR 的存储和数据处理并不是唯一可以外包给第三方云服务商的服务,医疗保健提供商通常会使用第三方计费服务来管理其结算费用和患者的健康保险.这是在实践中的典型场景:许多医生将计费外包给第三方提供商.这些计费服务累积了几个患者在不同的医疗保险方与医疗服务提供方的账单.从而导致隐私在这个模型中变得更加重要,因为健康保险或计费服务不应该访问 EHR 的私人详细信息.因此,对于 EHR 的隐私和安全设计变得极为重要,如表 7 所示,总结了基于不同技术的隐私安全设计方案.

Table 7 Security Encryption Based on Different Methods

表 7 基于不同技术的隐私安全设计

Method	Security System	Revocable	Cryptographic Correctness	Possible Problem
ABE	KP-ABE ^[99] , CP-ABE ^[100-103] , MA-ABE ^[104] , bABE ^[105] , EASiER ^[106]	Yes	Yes	Single Trustee
IBE	Revocable-IBE ^[107]	Yes	Yes	Slow Bilinear Group Calculation
HPE	APKS-Solution ^[96]	Yes	Yes	Low Search Performance
Domain Division	PUD ^[104]	Yes	Yes	Complex Domain
Opportunistic Computing	SPOC ^[108] , OC for WSN ^[109]	Yes	Yes	Device Power Problem
TVD	TVD with client platform ^[97,110-111]	Yes	No	Missing Emergency Access

5.2 基于属性加密的访问控制

基于属性加密,又被称为模糊的基于身份的加

密,是一种极具前景的支持细粒度访问的加密原语.不需要像身份加密一样,每次加密都必须知道接收

者的身份信息,在 ABE 中它把身份标识看做是一系列的属性.当用户拥有的属性超过加密者所描述的预设门槛时,用户是可以解密的.

Yu 等人^[99]、Boldyreva 等人^[107]、Ibraimi 等人^[100]使用 ABE 的方法来实现控制电子健康记录数据细粒度访问.得益于对于细粒度访问的支持,在 EHR 的隐私和安全问题上,ABE 得到了广泛的应用.

但是,以上方案存在共同的缺点.首先,它们通常假设使用单一系统中的受信任机构.这会造成负载瓶颈,同样也会遇到密钥托管方信任度的问题.因为受信任机构可以访问所有加密文件,这造成了隐私暴露的风险.此外,委派所有的属性管理任务(确认所有用户的属性或角色并生成密钥)到一个受信任机构是不切实际的.通常情况下,不同的组织一般对自己所在组织适用一套授权认证方式.例如,专业协会将负责认证医学专业资格,而健康服务提供方则负责认证其员工的工作级别.其次,仍然缺乏有效和按需撤销 ABE 的机制,这是确保 PHR 安全的重要组成部分.基于此,李琦等人^[112]提出了一个智慧健康环境下可追踪多授权机构基于属性的访问控制方案.该方案不仅支持多个授权机构,而且支持恶意用户追踪机制.

在目前的基于 ABE 的隐私安全控制中,大多数方法都没有区分个人和公共领域(personal and public domains, PUDs),这 2 者具有不同的属性定义、关键管理要求和可扩展性问题.Li 等人^[104]基于 PUDs 问题做出了相应研究,提出了一种在多领域中使用不同认证管理方式的架构.

5.3 可撤销 ABE

在 ABE 中有效且按需撤销用户或属性是一个众所周知的挑战性问题.传统方法中,这通常是由权威机构频繁地向未被撤销的用户周期性广播密钥更新^[101],这无法确保完全的后向与前向过程的安全性,而且效率较低.

Narayan 等人^[105]提出了一种在 EHR 系统上基于属性加密的基础架构,每个患者的 EHR 文件都是使用 ABE 变体 CP-ABE(密文协议属性加密)的加密方式,其特点在于允许直接撤销访问权限.同样地,Ibraimi 等人^[102]也将 CP-ABE 用于管理共享 PHR,并且引入了社会或专业领域的概念.Hur 等人^[103]和 Jahid 等人^[106]提出了 2 种具有直接属性撤销能力的 CP-ABE 方案,而不是周期性撤销.

可撤销 ABE 在密钥撤销的通信开销仍然很高,

因为它要求数据所有者将更新的密文组件发送给每个未经撤销的用户.

5.4 客户端安全

目前以上多数已有的分布式存储框架都是考虑到服务端的访问安全以及控制问题,而较少有涉及到客户端平台的安全.

可信虚拟域(trusted virtual domain, TVD)^[110-111]是一种被广泛使用的多域环境下的分布式安全框架,Löhr 等人^[97]基于 TVD 设计了一种安全框架,用以确保客户端以及外部数据存储的数据安全.

在移动可穿戴设备中,EHR 数据更新频率很快,通常需要 5min 就进行一次传输^[113],Lu 等人^[108]基于机会计算^[109,114]提出了一种安全且保护隐私的机会计算框架,用以保证移动可穿戴设备的客户端数据传输的安全性.

6 挑战和机遇

在深入调研智慧健康在云端、雾端、边缘以及隐私安全等方面的基础上,指出了智慧健康可能面临的六大挑战并提出了可以解决这些问题的技术机遇.

6.1 物端能耗和性能设计折中

在智慧健康服务的场景中,会存在大量医疗传感器分布在生活场所周围,这些传感器是智慧健康数据的源头,它们将源源不断地产生个人健康数据,并将这些数据发送到云、雾中.这些传感器的能耗成为整个系统的关键之处,若能耗过高,无法提供实时的、连续不断的服务,若性能过低,无法采集和处理足量的数据,也会影响到智慧健康服务的质量.如何去权衡传感器的能耗和性能成为了之后研究的一大关键点.低功耗的无线传输技术以及传感器技术将成为解决物端能耗和性能设计折衷的重要方法,未来将有更多的研究关注到低功耗无线传输技术和传感器技术.其次尽量减少在传感器节点的数据计算(如数据清洗、过滤和聚合等),也可以在保持低功耗的情况下实现高质量、快速响应的智慧健康服务,例如可以利用物联网智能网关和微型数据中心云辅助传感器节点进行数据处理.

6.2 异构化数据和多样化应用

目前,各类健康数据来自于各类不同的系统和形式各异的传感器,这些数据的结构和形式都不相同,这将导致服务需要对数据做大量的预处理工作,不仅影响服务的性能,也增加了出错的概率.因此,

数据的标准化和结构化是形成智慧健康大数据的必不可少的一环.为各类健康数据制定统一的数据格式标准是解决该问题的最根本、最直接的方法,但是由于长久以来存在各种各样独立的医疗系统,以及不同类型的医疗数据本就存在不同的数据形式,想在短期内实现异构化医疗数据的统一标准较为困难.在该情况下,如何使智慧健康后端系统去高性能地适应异构化数据成为了问题的关键,其中包含利用 NoSQL 数据库打破格式的限制、对异构化数据做结构化或半结构化处理、利用分布式技术加快预处理流程等.

6.3 医疗大数据感知的系统

在智慧健康的构建场景中,健康数据无时无刻在产生,并且这些健康数据还不同于一般的互联网大数据,健康大数据对于实时性的要求非常高,数据需要实时产生实时处理,并且由于个体移动性的特点,在不同的网络环境需要实现健康服务的移动感知.目前,采用云计算可以有效地处理大数据,但随着物联网的发展,数据量越来越大,云端也无法实时地处理健康数据,这时雾计算和边缘计算可以更好地满足健康数据实时性的要求,提高服务的性能.雾计算、边缘计算以及物联网技术是解决智慧健康应用实时性和移动感知的最佳方案之一.通过在云和传感器节点之间架设多样化的计算层,可以满足智慧健康服务实时性和移动感知的要求.特别是在即将到来的 5G 时代,健康数据规模变得更为庞大,雾计算、边缘计算和物联网技术构成的跨层次计算层对于智慧健康服务质量的提升极为关键.

6.4 个人数据隐私和安全

数据安全是永恒的话题,尽管智慧健康大数据可能有助于缓解许多与健康相关的问题,但其收集个人健康信息的能力可能会危及公民的隐私.保护隐私和基础设施安全是研究界仍在努力解决的不可避免的挑战.从收集的个人数据中可以判断出个人的生活习惯、家庭成员状态甚至于宗教信仰等隐私信息,这些信息非常敏感,特别是与健康息息相关.设计一个完善的保护公民隐私安全的机制成为了一大挑战.目前,基于属性加密方法以及可撤销 ABE 可以有效地控制对于健康数据的细粒度访问,并保证隐私安全.而区块链被认为是解决智慧健康数据隐私和安全的突破点,通过区块链来管理智慧健康数据,不仅可以实现健康数据共享,同时因为区块链的加密特性也很好地保证了隐私安全.

6.5 自适应的边缘资源融合

边缘设备面临独木不成林的问题,为了支撑日益复杂的现场智能应用,首先需要复杂边缘设备的协同.需要构建软件平台,实现对边缘计算资源的自主发现和自适应管理,尤其是借助区块链技术提供激励机制,以促进边缘设备计算资源融合.

6.6 高可靠高可用的系统设计

医疗健康场景对于高可靠性和高可用性有较高要求.需要研究高效的通信技术,以处理各类突发的数据拥塞;需要研究智能任务调度技术,以将关键任务按需分配到备份硬件上运行;需要实时的系统状态监控,以降低宕机风险的发生;需要分布式技术,通过副本机制来保证健康服务的可用性.

7 总 结

得益于云计算、雾计算和物联网技术的快速发展,关于智慧健康的研究日益增加.本文在调研大量近年来对于智慧健康领域的研究后,首先从云端出发,介绍了智慧健康大数据在云中的存储、检索和处理.然后从雾计算的角度,介绍了通过雾计算来增强智慧健康服务的各类研究.随后,从边缘出发,调研介绍了智慧健康服务的各类传感器和可穿戴设备,它们是数据产生的源头.最后,本文讨论区块链在智慧健康服务的诸多新兴应用以及智慧健康数据的隐私和安全问题,并提出了智慧健康服务的机遇与挑战,指出了物端能耗和性能设计折中、异构化数据和多样化应用、医疗大数据感知的系统、自适应的边缘资源融合、高可靠高可用的系统设计等未来热点研究方向.未来面向智慧健康的软硬件系统,尤其是跨越云和边的融合式设计将大有可为.

参 考 文 献

[1] Ahmed E, Yaqoob I, Gani A, et al. Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges [J]. IEEE Wireless Communications, 2016, 23(5): 10-16

[2] Kaisler S, Armour F, Espinosa J A, et al. Big data: Issues and challenges moving forward [C] //Proc of the 46th Hawaii Int Conf on System Sciences. Piscataway, NJ: IEEE, 2013: 995-1004

[3] Josep A D, Katz R, Konwinski A, et al. A view of cloud computing [J]. Communications of the ACM, 2010, 53(4): 50-58

- [4] Jadeja Y, Modi K. Cloud computing-concepts, architecture and challenges [C] //Proc of the Int Conf on Computing, Electronics and Electrical Technologies. Piscataway, NJ: IEEE, 2012: 877-880
- [5] Zhang Shuai, Zhang Shufen, Chen Xuebin, et al. Cloud computing research and development trend [C] //Proc of the 2nd Int Conf on Future Networks. Piscataway, NJ: IEEE, 2010: 93-97
- [6] Hou Xiaofeng, Song Pengtao, Tang Weichao, et al. Green hierarchical management for distributed datacenter containers [J]. Journal of Computer Research and Development, 2016, 53(7): 1493-1502 (in Chinese)
(侯小凤, 宋朋涛, 唐伟超, 等. 分布式集装箱数据中心的绿色层次化管理[J]. 计算机研究与发展, 2016, 53(7): 1493-1502)
- [7] Murdoch T B, Detsky A S. The inevitable application of big data to health care [J]. The Journal of the American Medical Association, 2013, 309(13): 1351-1352
- [8] Lin Chinho, Huang Liangcheng, Chou Sengcho, et al. Temporal event tracing on big healthcare data analytics [C] //Proc of the IEEE Int Congress on Big Data. Piscataway, NJ: IEEE, 2014: 281-287
- [9] Kaur K, Rani R. Managing data in healthcare information systems: Many models, one solution [J]. Computer, 2015, 48(3): 52-59
- [10] Yang Chaotung, Shih Wenchung, Chen Lungteng, et al. Accessing medical image file with co-allocation HDFS in cloud [J]. Future Generation Computer Systems, 2015, 43: 61-73
- [11] Guo Lejiang, Chen Fangxin, Chen Li, et al. The building of cloud computing environment for e-health [C] //Proc of the Int Conf on e-Health Networking Digital Ecosystems and Technologies. Piscataway, NJ: IEEE, 2010: 89-92
- [12] Chen Paoching, Freg Chihpin, Hou Tingwei, et al. Implementing RAID-3 on cloud storage for EMR system [C] //Proc of the Int Computer Symp. Piscataway, NJ: IEEE, 2010: 850-853
- [13] Fan Lu, Buchanan W, Thummler C, et al. DACAR platform for eHealth services cloud [C] //Proc of the 4th IEEE Int Conf on Cloud Computing. Piscataway, NJ: IEEE, 2011: 219-226
- [14] Chen Min, Mao Shiwen, Liu Yunhao. Big data: A survey [J]. Mobile Networks and Applications, 2014, 19(2): 171-209
- [15] White T. Hadoop: The Definitive Guide [M]. Sebastopol, CA: O'Reilly Media, 2012: 45-48
- [16] Natarajan K, Stein D, Jain S, et al. An analysis of clinical queries in an electronic health record search utility [J]. International Journal of Medical Informatics, 2010, 79(7): 515-522
- [17] Yang Lei, Mei Qiaozhu, Zheng Kai, et al. Query log analysis of an electronic health record search engine [C] //Proc of the American Medical Informatics Association Annual Symp. Bethesda, MD: AMIA, 2011: 915-924
- [18] Mu Xiangming, Lu Kun. Towards effective genomic information retrieval: The impact of query complexity and expansion strategies [J]. Journal of Information Science, 2010, 36(2): 194-208
- [19] Yang Yang. Attribute-based data retrieval with semantic keyword search for e-health cloud [J]. Journal of Cloud Computing, 2015, 4(1): 10-16
- [20] Zhang Lili, Zhang Yuqing, Liu Xuefeng, et al. Efficient conjunctive keyword search over encrypted electronic medical records [J]. Journal of Software, 2016, 27(6): 1577-1591 (in Chinese)
(张丽丽, 张玉清, 刘雪峰, 等. 对加密电子医疗记录有效的连接关键词的搜索[J]. 软件学报, 2016, 27(6): 1577-1591)
- [21] Yang Liu, Jin Rong, Mummert L, et al. A boosting framework for visually-preserving distance metric learning and its application to medical image retrieval [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010, 32(1): 30-44
- [22] Rahman M M, Bhattacharya P, Desai B C. A framework for medical image retrieval using machine learning and statistical similarity matching techniques with relevance feedback [J]. IEEE Transactions on Information Technology in Biomedicine, 2007, 11(1): 58-69
- [23] Cabarcos A, Sanchez T, Seoane J A, et al. Retrieval and management of medical information from heterogeneous sources, for its integration in a medical record visualisation tool [J]. International Journal of Electronic Healthcare, 2010, 5(4): 371-385
- [24] Kim J, Feng Dagan, Cai Wendong, et al. Integrated multimedia medical data agent in e-Health [C] //Proc of the Pan-Sydney Area Workshop on Visual Information. Darlinghurst, SYD: Australian Computer Society, 2001: 11-15
- [25] Shen Chiaping, Chen Weihsin, Chen Jiaming, et al. Bio-signal analysis system design with support vector machines based on cloud computing service architecture [C] //Proc of the Annual Int Conf of the IEEE Engineering in Medicine and Biology. Piscataway, NJ: IEEE, 2010: 1421-1424
- [26] Takeuchi H, Kodama N. Validity of association rules extracted by healthcare-data-mining [C] //Proc of the 36th Annual Int Conf of the IEEE Engineering in Medicine and Biology Society. Piscataway, NJ: IEEE, 2014: 4960-4963
- [27] Kurt I, Ture M, Kurum A T. Comparing performances of logistic regression, classification and regression tree, and neural networks for predicting coronary artery disease [J]. Expert Systems with Applications, 2008, 34(1): 366-374
- [28] Nkosi M T, Mekuria F. Cloud computing for enhanced mobile health applications [C] //Proc of the 2nd IEEE Int Conf on Cloud Computing Technology and Science. Piscataway, NJ: IEEE, 2010: 629-633
- [29] Wang Xiaoliang, Gui Qiong, Liu Bingwei, et al. Enabling smart personalized healthcare: A hybrid mobile-cloud approach for ECG telemonitoring [J]. IEEE Journal of Biomedical and Health Informatics, 2014, 18(3): 739-745

- [30] Hsieh J, Hsu M W. A cloud computing based 12-lead ECG telemedicine service [J]. BMC Medical Informatics and Decision Making, 2012, 12(1): 77-88
- [31] Parkka J, Ermes M, Korpipaa P, et al. Activity classification using realistic data from wearable sensors [J]. IEEE Transactions on Information Technology in Biomedicine, 2006, 10(1): 119-128
- [32] Leonov V. Thermoelectric energy harvesting of human body heat for wearable sensors [J]. IEEE Sensors Journal, 2013, 13(6): 2284-2291
- [33] Poon C C Y, Zhang Yuanting. Cuff-less and noninvasive measurements of arterial blood pressure by pulse transit time [C] //Proc of the 27th IEEE Annual Conf Engineering in Medicine and Biology. Piscataway, NJ: IEEE, 2006: 5877-5880
- [34] Tamura T, Maeda Y, Sekine M, et al. Wearable photoplethysmographic sensors—Past and present [J]. Electronics, 2014, 3(2): 282-302
- [35] Baek H J, Chung G S, Kim K K, et al. Photoplethysmography measurement without direct skin-to-sensor contact using an adaptive light source intensity control [J]. IEEE Transactions on Information Technology in Biomedicine, 2009, 13(6): 1085-1088
- [36] Poh M Z, McDuff D J, Picard R W. Advancements in noncontact, multiparameter physiological measurements using a webcam [J]. IEEE Transactions on Biomedical Engineering, 2011, 58(1): 7-11
- [37] Baek H J, Chung G S, Kim K K, et al. A smart health monitoring chair for noninvasive measurement of biological signals [J]. IEEE Transactions on Information Technology in Biomedicine, 2012, 16(1): 150-158
- [38] Lanatà A, Scilingo E P, Nardini E, et al. Comparative evaluation of susceptibility to motion artifact in different wearable systems for monitoring respiratory rate [J]. IEEE Transactions on Information Technology in Biomedicine, 2010, 14(2): 378-386
- [39] Zhang Zhengbo, Shen Yuhong, Wang Weidong, et al. Design and implementation of sensing shirt for ambulatory cardiopulmonary monitoring [J]. Journal of Medical and Biological Engineering, 2011, 31(3): 207-215
- [40] Shany T, Redmond S J, Narayanan M R, et al. Sensors-based wearable systems for monitoring of human movement and falls [J]. IEEE Sensors Journal, 2012, 12(3): 658-670
- [41] Kan Yaochiang, Chen Chunkai. A wearable inertial sensor node for body motion analysis [J]. IEEE Sensors Journal, 2012, 12(3): 651-657
- [42] Huang Zheng, Han Lixin, Xiao Yan. A new step approach based on mobile termination [J]. Chinese Journal of Computers, 2017, 40(8): 1856-1871 (in Chinese)
(黄政, 韩立新, 肖艳. 一种基于移动终端的新型计步方法 [J]. 计算机学报, 2017, 40(8): 1856-1871)
- [43] Bonomi F, Milito R, Zhu Jiang, et al. Fog computing and its role in the Internet of things [C] //Proc of the 1st Edition of the MCC Workshop on Mobile Cloud Computing. New York: ACM, 2012: 13-16
- [44] Li Chao, Xue Yushu, Wang Jing, et al. Edge-oriented computing paradigms: A survey on architecture design and system management [J]. ACM Computing Surveys, 2018, 51(2): 39-73
- [45] Song Pengtao, Li Chao, Xu Liting, et al. Edge computing system for smart home based on personal computer [J]. Computer Engineering, 2017, 43(11): 1-7 (in Chinese)
(宋朋涛, 李超, 徐莉婷, 等. 基于个人计算机的智能家居边缘计算系统 [J]. 计算机工程, 2017, 43(11): 1-7)
- [46] Zhu Qian, Wang Ruicong, Chen Qi, et al. IoT gateway: Bridging wireless sensor networks into Internet of things [C] //Proc of the IEEE/IFIP Int Conf on Embedded and Ubiquitous Computing. Piscataway, NJ: IEEE, 2010: 347-352
- [47] Emara K A, Abdeen M, Hashem M. A gateway-based framework for transparent interconnection between WSN and IP network [C] //Proc of the IEEE Int Conf on Smart Technologies. Piscataway, NJ: IEEE, 2009: 1775-1780
- [48] Mueller R, Rellermeier J S, Duller M, et al. A generic platform for sensor network applications [C] //Proc of the IEEE Int Conf on Mobile Adhoc and Sensor Systems. Piscataway, NJ: IEEE, 2007: 1-3
- [49] Bimschas D, Hellbrück H, Mietz R, et al. Middleware for smart gateways connecting sensornets to the Internet [C] //Proc of the 5th Int Workshop on Middleware Tools, Services and Run-Time Support for Sensor Networks. New York: ACM, 2010: 8-14
- [50] Shang Guoqiang, Chen Yanming, Zuo Chao, et al. Design and implementation of a smart IoT gateway [C] //Proc of the IEEE Int Conf on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing. Piscataway, NJ: IEEE, 2013: 720-723
- [51] Stantchev V, Barnawi A, Ghulam S, et al. Smart items, fog and cloud computing as enablers of servitization in healthcare [J]. Sensors & Transducers, 2015, 185(2): 121-128
- [52] Quwaider M, Jararweh Y. Cloudlet-based for big data collection in body area networks [C] //Proc of the 8th Int Conf for Internet Technology and Secured Transactions. Piscataway, NJ: IEEE, 2013: 137-141
- [53] Lo'ai A T, Bakhader W, Mehmood R, et al. Cloudlet-based mobile cloud computing for healthcare applications [C] //Proc of the IEEE Global Communications Conf. Piscataway, NJ: IEEE, 2016: 1-6
- [54] Chen Min, Qian Yongfeng, Chen Jing, et al. Privacy protection and intrusion avoidance for cloudlet-based medical data sharing [J]. IEEE Transactions on Cloud Computing, 2016, 2(4): 2529-2533

- [55] El Amraoui A, Sethom K. Cloudlet softwarization for pervasive healthcare [C] //Proc of the 30th Int Conf on Advanced Information Networking and Applications Workshops. Piscataway, NJ: IEEE, 2016: 628-632
- [56] Lee JinShyan, Su Yuwei, Shen Chungchou. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and WiFi [J]. Industrial Electronics Society, 2007, 5(8): 46-51
- [57] Navya K, Murthy M B R. A ZigBee based patient health monitoring system [J]. Journal of Engineering Research and Applications, 2013, 3(5): 483-486
- [58] Kim Y, Lee S S, Lee S K. Coexistence of ZigBee-based WBAN and WiFi for health telemonitoring systems [J]. IEEE Journal of Biomedical and Health Informatics, 2016, 20(1): 222-230
- [59] Curtis A R, Mogul J C, Tourrilhes J, et al. DevoFlow: Scaling flow management for high-performance networks [C] //Proc of the ACM SIGCOMM Conf. New York: ACM, 2011: 254-265
- [60] Omre A H, Keeping S. Bluetooth low energy: Wireless connectivity for medical monitoring [J]. Journal of Diabetes Science and Technology, 2010, 4(2): 457-463
- [61] Laine T H, Lee C, Suk H. Mobile gateway for ubiquitous health care system using zigbee and bluetooth [C] //Proc of the 8th Int Conf on Innovative Mobile and Internet Services in Ubiquitous Computing. Piscataway, NJ: IEEE, 2014: 139-145
- [62] Al-Tae M A, Jaradat N A, Ali D M A. Mobile phone-based health data acquisition system using Bluetooth technology [C] //Proc of the IEEE Jordan Conf on Applied Electrical Engineering and Computing Technologies (AEECT). Piscataway, NJ: IEEE, 2011: 1-6
- [63] Khan U M, Kabir Z, Hassan S A. Wireless health monitoring using passive WiFi sensing [C] //Proc of the 13th Int Wireless Communications and Mobile Computing Conf. Piscataway, NJ: IEEE, 2017: 1771-1776
- [64] Tan Bo, Chen Qingchao, Chetty K, et al. Exploiting WiFi channel state information for residential healthcare informatics [J]. IEEE Communications Magazine, 2018, 56(5): 130-137
- [65] Zhang Fan, Zhang Yanqing, Silver J, et al. A batteryless 19 μ W MICS/ISM-band energy harvesting body area sensor node SoC [C] //Proc of the IEEE Int Solid-State Circuits Conf. Piscataway, NJ: IEEE, 2012: 298-300
- [66] Cho N, Bae J, Yoo H J. A 10.8mW body channel communication/MICS dual-band transceiver for a unified body sensor network controller [J]. IEEE Journal of Solid-State Circuits, 2009, 44(12): 3459-3468
- [67] Yoo J, Yan Long, Lee S, et al. A 5.2 mW self-configured wearable body sensor network controller and a 12 μ W 54.9% efficiency wirelessly powered sensor for continuous health monitoring system [C] //Proc of the IEEE Int Solid-State Circuits Conf. Piscataway, NJ: IEEE, 2009: 290-300
- [68] Gope P, Hwang T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network [J]. IEEE Sensors Journal, 2016, 16(5): 1368-1376
- [69] Bao Shudi, Poon C C Y, Zhang Yuanting, et al. Using the timing information of heartbeats as an entity identifier to secure body sensor network [J]. IEEE Transactions on Information Technology in Biomedicine, 2008, 12(6): 772-779
- [70] Fortino G, Giannantonio R, Gravina R, et al. Enabling effective programming and flexible management of efficient body sensor network applications [J]. IEEE Transactions on Human-Machine Systems, 2013, 43(1): 115-133
- [71] Lo B P L, Thiemjarus S, King R, et al. Body sensor network—A wireless sensor platform for pervasive healthcare monitoring [C] //Proc of the 3rd Int Conf on Pervasive Computing. Berlin: Springer, 2005: 70-88
- [72] Hossain M S, Muhammad G. Cloud-assisted industrial Internet of things (IIoT)—Enabled framework for health monitoring [J]. Computer Networks, 2016, 101: 192-202
- [73] Muhammad G, Rahman S K M M, Alelaiwi A, et al. Smart health solution integrating IoT and cloud: A case study of voice pathology monitoring [J]. IEEE Communications Magazine, 2017, 55(1): 69-73
- [74] Lin Borshing, Chou Naikuan, Chong Fokching, et al. RTWPMS: A real-time wireless physiological monitoring system [J]. IEEE Transactions on Information Technology in Biomedicine, 2006, 10(4): 647-656
- [75] Sun Mingui, Burke L E, Mao Zhihong, et al. eButton: A wearable computer for health monitoring and personal assistance [C] //Proc of the 51st Annual Design Automation Conf. New York: ACM, 2014: 1-6
- [76] Melillo P, Orrico A, Scala P, et al. Cloud-based smart health monitoring system for automatic cardiovascular and fall risk assessment in hypertensive patients [J]. Journal of Medical Systems, 2015, 39(10): 109-115
- [77] Leijdekkers P, Gay V. A self-test to detect a heart attack using a mobile phone and wearable sensors [C] //Proc of the 21st IEEE Int Symp on Computer-Based Medical Systems. Piscataway, NJ: IEEE, 2008: 93-98
- [78] Pandian P S, Mohanavelu K, Safeer K P, et al. Smart vest: Wearable multi-parameter remote physiological monitoring system [J]. Medical Engineering & Physics, 2008, 30(4): 466-477
- [79] Di Rienzo M, Rizzo F, Parati G, et al. MagIC system: A new textile-based wearable device for biological signal monitoring. Applicability in daily life and clinical setting [C] //Proc of the 27th IEEE Engineering in Medicine and Biology Annual Conf. Piscataway, NJ: IEEE, 2005: 7167-7169
- [80] Wang Aosen, Chen Lizhong, Xu Wen Yao. XPro: A cross-end processing architecture for data analytics in wearables [C] //Proc of the 44th Annual Int Symp on Computer Architecture. New York: ACM, 2017: 69-80

- [81] Mohammed J, Lung C H, Ocneanu A, et al. Internet of things: Remote patient monitoring using Web services and cloud computing [C] //Proc of the IEEE Int Conf on Internet of Things. Piscataway, NJ: IEEE, 2014: 256-263
- [82] Sebestyen G, Hangan A, Oniga S, et al. eHealth solutions in the context of Internet of things [C] //Proc of the IEEE Int Conf on Automation, Quality and Testing, Robotics. Piscataway, NJ: IEEE, 2014: 1-6
- [83] Wu Xindong, Ye Mingquan, Hu Donghui, et al. Pervasive medical information management and services: Key techniques and challenges [J]. Chinese Journal of Computers, 2012, 35 (5): 827-845 (in Chinese)
(吴信东, 叶明全, 胡东辉, 等. 普适医疗信息管理与服务的关键技术与挑战[J]. 计算机学报, 2012, 35(5): 827-845)
- [84] Böhme R, Christin N, Edelman B, et al. Bitcoin: Economics, technology, and governance [J]. Journal of Economic Perspectives, 2015, 29(2): 213-238
- [85] Dagher G G, Mohler J, Milojkovic M, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology [J]. Sustainable Cities and Society, 2018, 39: 283-297
- [86] Liang Xueping, Zhao Juan, Shetty S, et al. Integrating blockchain for data sharing and collaboration in mobile healthcare applications [C] //Proc of the 28th IEEE Annual Int Symp on Personal, Indoor, and Mobile Radio Communications. Piscataway, NJ: IEEE, 2017: 1-5
- [87] Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus [EB/OL]. (2018-04-25) [2019-06-21]. <http://journals.sagepub.com/doi/abs/10.1177/1460458218769699>
- [88] Azaria A, Ekblaw A, Vieira T, et al. Medrec: Using blockchain for medical data access and permission management [C] //Proc of the 2nd Int Conf on Open and Big Data. Piscataway, NJ: IEEE, 2016: 25-30
- [89] Kuo T T, Ohno-Machado L. ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks [J]. arXiv preprint arXiv: 1802.01746, 2018
- [90] Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality [J]. Trials, 2017, 18(1): 335-340
- [91] Taylor P. Applying blockchain technology to medicine traceability [EB/OL]. (2016-04-27) [2019-06-21]. http://www.securindingustry.com/pharmaceuticals/applying-blockchain-technology-to-medicine-traceability/s40/a2766/#.XQ7jjG8zY_V
- [92] Schöner M M, Kourouklis D, Sandner P, et al. Blockchain technology in the pharmaceutical industry [EB/OL]. (2017-07-01) [2019-06-21]. http://explore-ip.com/2017_Blockchain-Technology-in-the-Pharmaceutical-Industry.pdf
- [93] Prisco G. The blockchain for healthcare: Gem launches gem health network with philips blockchain lab [EB/OL]. (2016-04-26) [2019-06-21]. <http://bitcoinmagazine.com/articles/the-blockchain-for-healthcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938>
- [94] Williams-Grut O. Estonia is using the technology behind bitcoin to secure 1 million health records [EB/OL]. (2016-03-03) [2019-06-23]. <http://www.businessinsider.com/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3>
- [95] Witchey N J. Healthcare transaction validation via blockchain proof-of-work, systems and methods: United States, US20150332283A1 [P]. 2015-11-19
- [96] Li Ming, Yu Shucheng, Cao Ning, et al. Authorized private keyword search over encrypted data in cloud computing [C] //Proc of the 31st Int Conf on Distributed Computing Systems. Piscataway, NJ: IEEE, 2011: 383-392
- [97] Löhr H, Sadeghi A R, Winandy M. Securing the e-health cloud [C] //Proc of the 1st ACM Int Health Informatics Symp. New York: ACM, 2010: 220-229
- [98] Mandl K D, Markwell D, MacDonald R, et al. Public standards and patients' control: How to keep electronic medical records accessible but private [J]. British Medical Journal, 2001, 322(7281): 283-287
- [99] Yu Shucheng, Wang Cong, Ren Kui, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing [C] //Proc of the IEEE Int Conf on Computer Communications. Piscataway, NJ: IEEE, 2010: 534-542
- [100] Ibraimi L, Petkovic M, Nikova S, et al. Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes [R]. Enschede, Netherland: University of Twente, 2009
- [101] Liang Xiaohui, Lu Rongxing, Lin Xiaodong, et al. Ciphertext policy attribute based encryption with efficient revocation [R]. Waterloo, Ontario, Canada: University of Waterloo, 2010
- [102] Ibraimi L, Asim M, Petkovi M. Secure management of personal health records by applying attribute-based encryption [C] //Proc of the 6th Int Workshop on Wearable, Micro, and Nano Technologies for Personalized Health. Piscataway, NJ: IEEE, 2009: 71-74
- [103] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22 (7): 1214-1221
- [104] Li Ming, Yu Shucheng, Zheng Yao, et al. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1): 131-143
- [105] Narayan S, Gagné M, Safavi-Naini R. Privacy preserving EHR system using attribute-based infrastructure [C] //Proc of the ACM Workshop on Cloud Computing Security. New York: ACM, 2010: 47-52
- [106] Jahid S, Mittal P, Borisov N. EASiER: Encryption-based access control in social networks with efficient revocation [C] //Proc of the 6th ACM Symp on Information, Computer and Communications Security. New York: ACM, 2011: 411-415

[107] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation [C] //Proc of the 15th ACM Conf on Computer and Communications Security. New York: ACM, 2008: 417-426

[108] Lu Rongxing, Lin Xiaodong, Shen Xueming. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24 (3): 614-624

[109] Avvenuti M, Corsini P, Masci P, et al. Opportunistic computing for wireless sensor networks [C] //Proc of the IEEE Int Conf on Mobile Adhoc and Sensor Systems. Piscataway, NJ: IEEE, 2007: 1-6

[110] Bussani A, Griffin J L, Jansen B, et al. Trusted virtual domains: Secure foundations for business and IT services, RC23792 [R]. Almaden, CA: IBM Research, 2005

[111] Cabuk S, Dalton C I, Eriksson K, et al. Towards automated security policy enforcement in multi-tenant virtual data centers [J]. Journal of Computer Security, 2010, 18(1): 89-121

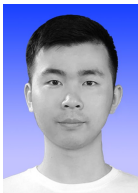
[112] Li Qi, Zhu Hongbo, Xiong Jinbo, et al. Multi-authority attribute-based access control system in mHealth with traceability [J]. Journal on Communications, 2018, 39(6): 1-10 (in Chinese)
(李琦, 朱洪波, 熊金波, 等. mHealth 中可追踪多授权机构基于属性的访问控制方案 [J]. 通信学报, 2018, 39(6): 1-10)

[113] Yuce M R, Ng S W P, Myo N L, et al. Wireless body sensor network using medical implant band [J]. Journal of Medical Systems, 2007, 31(6): 467-474

[114] Passarella A, Conti M, Borgia E, et al. Performance evaluation of service execution in opportunistic computing [C] //Proc of the 13th ACM Int Conf on Modeling, Analysis, and Simulation of Wireless and Mobile Systems. New York: ACM, 2010: 291-298



Qiu Yu, born in 1993. Master candidate. His main research interests include cloud computing, smart health, distributed system and parallel computing.



Wang Chi, born in 1997. Master candidate. His main research interests include parallel computing and machine learning.



Qi Kaiyue, born in 1977. Associate professor at Shanghai Jiao Tong University. His main research interests include information security and big data.



Shen Yao, born in 1975. Associate professor at Shanghai Jiao Tong University. His main research interests include cloud computing, distributed systems and deep learning.



Li Chao, born in 1986. Tenure-track associate professor at Shanghai Jiao Tong University. Member of CCF. His main research interests include computer architecture and systems.



Zhang Chengmi, born in 1985. Attending doctor at Xinhua Hospital Affiliated to Shanghai Jiao Tong University School of Medicine. His main research interests include mechanisms, prevention and treatment of perioperative respiratory complications. (zhcm1985@sina.com)



Guo Minyi, born in 1962. Professor at Shanghai Jiao Tong University. IEEE fellow. His main research interests include parallel and distributed processing, parallelizing compilers and cloud computing.