DOI:10.7544/issn1000-1239.2016.********
卷(期):起止页,年

面向可穿戴设备的数据安全隐私保护技术综述

刘强　李桐　于洋　蔡志平　周桐庆

（国防科学技术大学计算机学院 长沙 410073）

（qiangliu06@nudt.edu.cn）

Data Security and Privacy Preserving Techniques for Wearable Devices: A Survey

Liu Qiang, Li Tong, Yu Yang, Cai Zhiping, and Zhou Tongqing

（*College of Computer, National University of Defense Technology, Changsha 410073*）

Abstract Mobile computing based on wearable devices is considered as the important technology for supporting ubiquitous perceptual applications. It uses widespread sensors to continuously sense the environment information. Moreover, it also adopts short-range communication and data mining/machine learning to transmit and process the sensed data, respectively. Current work mainly focuses on designing and implementing new mobile applications, information gathering, product modality and friendly user interfaces. However, research on data security and privacy technology for wearable devices is still in its fancy. In the perspective of data analysts, researchers analyze characteristics of diverse data in wearable devices and privacy threats targeting wearable devices. Moreover, they are particularly interested in human activity recognition techniques and data mining mechanisms based on multi-source sensing data. On the other hand, it is vital for privacy protectors of wearable devices to study on privacy preservation techniques in the following three aspects: cloud-assisted privacy preserving mechanisms, privacy-aware personal data publishing and policy-based access control. A case study regarding security and privacy for Fitbit, a kind of wearable devices for health tracking, is presented. At last, the technological approaches to preserve data security and privacy for wearable devices are summarized, and some open issues to be further studied are also raised.

Key words mobile computing; wearable devices; data security and privacy; security threat; privacy preservation

摘要　基于可穿戴设备的移动计算被视为支撑泛在感知型应用的重要技术，它使用大范围部署的传感器持续不断地感知环境信息，利用短距通信和数据挖掘/机器学习技术传递和处理感知数据．现有的可穿戴设备相关工作主要关注新型移动应用、信息采集、产品形态和人性化用户接口等方面的设计与实现．然而，面向可穿戴设备的数据安全隐私保护技术研究尚处于起步阶段．从数据分析者的视角来看，研究者分析可穿戴设备的数据源特点与隐私安全隐患，重点研究基于多源感知数据的个体活动识别方法和数据挖掘机制；从隐私安全保护者的视角来看，面向可穿戴设备的隐私保护技术亟需解决云辅助的隐私保护机制、隐私感知的个人信息发布和基于策略的访问控制等方面的问题．以可穿戴健康跟踪设备 Fitbit 为对象展开了可穿戴设备安全与隐私实例分析．最后，总结了面向可穿戴设备的隐私保护的几条技术途径，并展望了需要进一步研究的热点问题．

收稿日期：2016-10-17；**修回日期**：2016-**-**
基金项目：国家自然科学基金项目（61379145, 61363071）
This work is supported by the National Natural Science Foundation of China (61379145, 61363071).
通信作者：蔡志平（zpcai@nudt.edu.cn）

关键词 移动计算；可穿戴设备；数据安全与隐私；安全威胁；隐私保护

中图法分类号 TP309.2

随着微电子技术、计算机技术和现代无线通信技术的高速发展，可穿戴设备具有许多新特点，比如更强的计算能力、更大的存储空间、更高的数据传输速率、更小设备规格、更低的成本以及更加友好的人机交互能力等．另一方面，可穿戴设备内部集成的传感器类型日趋多样化，包括陀螺仪、加速计、麦克风、数字罗盘和摄像头等．基于这些可穿戴传感器，大量感知型应用方兴未艾，极大地便利了人们的日常生活，也深刻地影响着人们的生活习惯．例如，群智感知(Crowd Sensing)是一类典型的感知型应用，用户采集自身的行为数据和周边环境的信息，随后通过互联的网络将感知数据上传给应用服务器[1]．应用服务器处理接收到的感知数据、提取出查询者感兴趣的关键信息并将查询结果发送给查询者．群智感知的应用案例有微博、移动社交网络[2]、个人健康监控[3]等等．

近年来，虽然可穿戴设备相关学术研究和产业推广均得到了长足进步[4]，但是现有的工作主要关注新型移动应用的设计与研发、数据采集技术的研究与部署、产品形态和人机交互的人性化设计与实现等内容，而在设备拥有者隐私保护方面尚未形成统一且标准的做法[5]．随着可穿戴设备的日益普及，可穿戴设备隐私安全相关事件也时常见报．例如，2014 年，多家媒体报道在国外某马拉松比赛现场，研究者曾通过蓝牙嗅探设备在起跑线和终点线共记录了 563 个不同设备的信息，获取到了大量未被加密的健康信息，并通过设备物理地址和广播的设备名定位到了具体的设备和佩戴者；2015 年，卡巴斯基实验室安全研究专家通过对多种健康手环同智能手机之间的互动进行检测，结果显示多种常见的智能手环所使用的验证手段都允许第三方隐身连接至这些可穿戴设备并执行命令；国内著名的乌云平台在 2015 年底公开了两个与儿童智能手表相关的安全漏洞，它们分别是一米阳光儿童智能手表 G1 任意绑定漏洞(WooYun-2015-143456)和开咪儿童智能手表恶意绑定未出售设备漏洞(WooYun-2015-143611)，这些安全漏洞给用户带来了严峻的隐私安全问题和设备可用性问题．另一方面，来自广大地理范围内的各类感知数据不可避免地蕴含着用户的大量时间和空间信息[1]．一旦这些数据被组织起来并加以分析，单用户的个人信息以及多用户的关联信息将面临被泄露的风险[6,7]．此外，恶意攻击者有意监测和捕获合法用户之间的交互信息也将极大地破坏用户隐私[8-14]．除了可穿戴设备拥有者的隐私面临着严峻挑战，海量感知数据的安全与隐私问题也是影响可穿戴设备普及应用的另一个主要因素[15,16]．以电子健康医务应用为例，泛在健康状态监控、远程医疗救助、紧急医疗响应等典型功能要求目标患者身上的可穿戴传感器持续地采集关键体征和活动数据，并通过短距无线通信技术(比如无线体域网)相互通信．然而，受限于可穿戴传感器有限的计算能力与存储空间，电子健康医务面临着两大数据安全挑战：(1)分布式数据存储安全(比如保密性、动态完整性保护、可靠性等)；(2)针对患者的敏感医疗数据的分布式数据访问安全(比如细粒度的数据访问控制、敏捷数据访问、可审计、不可抵赖等)[17]．综上所述，面向可穿戴设备的数据安全与隐私保护是未来较长时间内的热门研究领域，其中，泛在数据的感知及其关联分析和可穿戴设备数据的安全访问是亟需解决的两大关键科学问题．

本文围绕面向可穿戴设备的数据安全隐私保护技术主题(“一个主题”)，以上述两大关键科学问题为出发点，从针对可穿戴设备数据的安全威胁和面向可穿戴设备的数据安全与隐私保护技术两个主要方面(“两条主线”)梳理现有研究工作，如图 1 所示．在针对可穿戴设备数据的安全威胁方面，本文归纳了可穿戴设备数据的来源、特性和类型，进而分析了可穿戴设备面临的各类隐私安全威胁，梳理了给可穿戴设备数据隐私安全带来潜在威胁的个体活动识别方法和数据挖掘机制；在面向可穿戴设备的数据安全与隐私保护技术方面，本文分别归纳了云辅助的隐私保护机制、隐私感知的个人信息发布机制和基于策略的访问控制机制等三个方面的研究工作．

本文第 1 节从数据分析者的视角重点分析可穿戴设备中数据的特点及其面临的隐私安全隐患，进而从基于泛在感知数据的个体活动识别方法和面向个人行为分析的数据挖掘机制两个方面梳理可穿戴设备中面向可穿戴设备的泛在数据分析相关工作．第 2 节从隐私安全保护者的视角着重在云辅助的隐私保护机制、隐私感知的个人信息发布机制和基于访问控制的隐私保护机制三个热门研究方向介绍面向可穿戴设备的隐私保护技术相关研究成果．第 3 节以可穿戴健康跟踪设备 Fitbit 为对象展开了可穿戴设备数据安全与隐私保护实例分析．第 4 节展望了面向可穿戴设备的数据安全隐私保护技术的热点和趋势．

1 针对可穿戴设备数据的安全威胁

1.1 可穿戴设备中数据的特点

在可穿戴计算环境中，多源异构数据主要来自传感器数据源和非传感器数据源，其中传感器数据源主要采集环境上下文信息、用户生理信息、位置信息．表 1 从数据源类型、数据源特性、数据来源和数据类型等四个方面汇总了不同数据源的相关细节．

1.2 可穿戴设备中数据面临的隐私安全隐患

从数据分析者角度看，可穿戴数据的敏感性与重要性使得可穿戴设备面临着多种隐私安全威胁．例如，心率、血糖等健康数据涉及到用户的健康状况，

Table 1 A summary of sources and characteristics of data in wearable devices

表 1 可穿戴设备中的数据源及其特点

Type of Data Source	Characteristic	Data Source	Data Type
Sensing data source	Physiological data	Heart-rate monitor	Numeric / Integer
		Blood glucose monitor	Numeric / Integer
	Body activity	Accelerator	Numeric / Float
	Environment	Temperature	Numeric / Float
		Humidity	Numeric / Integer
		Atmospheric pressure monitor	Numeric / Float
	Navigation	GPS location	Numeric / Float
		Compass	Text
User interactive data source	Input	Touch and key stroking	Test / Numeric
		Microphone	Audio
		Camera	Picture / Video
Data source in devices	Application logs	Web logs	Text
		Application related logs	Text
	Communication logs	Bluetooth scanning	Text
		Wi-Fi scanning	Text
	User data	Contact list	Text
		Call history	Text
		Short message service (SMS) data	Text

Table 2 Vulnerability analysis on privacy and security of wearable devices

表 2 可穿戴设备中的隐私安全隐患分析

Type of Data Source	Characteristic	Security & Privacy Threat	Affected Function
Sensing data source	Physiological data	Healthy data leakage	Information; publishing; communication; access control
	Body activity	User tracking, user habit analysis	
	Environment	User environment information leakage	
	Navigation	Location based inferring attack, physical location leakage, user identity attack, sensitive location tracking, user trajectory tracking	
User interactive data source	Input	Peeping, eavesdropping, illegal access of third-party applications	Access control
Data source in devices	Application logs	IP information leakage, traffic analysis, communication sniffer	Communication
	Communication logs	Location leakage, stealing sensitive information	Communications; access control
	User data	User identity attack	access control

其泄露可能导致歧视、诈骗等一系列社会问题. 表 2 归纳了可穿戴设备中的各类隐私安全隐患. 不同类型的数据源面临着不同的隐私安全隐患，具体分析过程如下：

1.2.1 传感器数据源面临的隐私安全隐患

由于可穿戴传感器的类型多样（例如生理数据、身体活动数据、环境数据、导航数据等等），因此相应的数据源特性也不尽相同：(1)生理数据源面临着健康数据泄露的隐私安全隐患. 攻击者通过分析目标用户的心率、血糖等健康数据，就可以分析出用户的健康指数. 如果该用户被泄露的健康情况是一些难以启齿的疾病（比如艾滋病、乙肝等），那么他有可能受到歧视或不公平的待遇. (2)身体活动数据源面临着用户运动轨迹跟踪、用户生活习惯分析等的隐私安全隐患. 攻击者通过恶意程序可以读取加速计信息，进而分析加速计数据以跟踪用户运动轨迹；通过关联不同用户的身体活动数据，攻击者能够分析出目标用户的生活习惯信息，例如每天在非工作时间同时乘坐地铁的两个人可能存在某种关系等. (3)环境数据源面临着用户生活环境信息泄露的隐私安全隐患. 攻击者通过分析目标用户所处环境的温度、湿度及气压等数据，可推测该用户的生活环境信息，例如室内/室外. (4)导航数据源面临着基于位置信息的推断攻击、物理位置信息泄漏、用户身份攻击、敏感位置定位、用户行动轨迹追踪等的隐私安全隐患. 攻击者根据不同空间位置上感知任务的执行情况推断出与位置信息相关的敏感信息，例如对于一个大规模爆发的群体性事件，虽然单个用户可以通过匿名的方式向应用服务器上传周边事态数据，但是攻击者仍然可以关联分析不同用户的位置信息来推断事态紧急程度等重要信息；攻击者也可以利用多个用户位置数据之间的强关联性来挖掘其群体性隐私信息.

1.2.2 用户交互数据源面临的隐私安全隐患

用户交互数据源主要体现了输入数据特性，而输入数据面临着偷窥、窃听、偷拍、第三方应用非法访问等的隐私安全隐患. 攻击者可以非法获取目标用户

通过触屏、键盘、麦克风、摄像头所产生的文本、声音、图片和视频等数据.

1.2.3 设备内部数据源面临的隐私安全隐患

设备内部数据主要包括应用日志数据、通信日志数据和用户数据等：(1)应用日志数据源面临着 IP 地址信息泄露、流量分析、通信窃听等的隐私安全隐患. 攻击者通过应用相关日志可以获取用户的应用记录，例如搜索的关键词、购物记录等. (2)通信日志数据面临着位置信息泄露和用户重要信息窃取等的隐私安全隐患. 由于许多可穿戴设备通过 Wi-Fi 或蓝牙与手机设备相连，攻击者可以分析通信数据来非法获取手机上的重要数据，例如通话记录、短信内容等. (3)用户数据源面临着用户身份攻击的隐私安全风险. 攻击者可以窃取目标用户的通讯录、通话记录和短信等敏感信息，以获取对用户不利的隐私信息.

1.3 基于泛在感知数据的个体活动识别方法

近年来，泛在感知(Ubiquitous Sensing)是传感器网络研究领域中的一个新兴研究方向，泛在感知这一概念试图构建一个分布式的、互联的计算基础设施以透明地支持用户活动. 具体来说，泛在感知利用传感技术所提供的感知能力来实现泛在计算基础设施，其中多种传感器所组成的传感网络能够产生丰富的多模态传感数据流. 另一方面，针对传感数据的分析可以确定环境特性以及为分布式的用户与环境提供相互交互的上下文. 随着可穿戴设备的广泛普及，人们能够借助泛在感知技术，从可穿戴传感数据中识别出典型的日常活动（例如行走、跑步、跳跃、坐下、站立、躺下等等），从而帮助形成更为健康的生活习惯[18]. 个体活动识别(Human Activity Recognition, HAR)技术在基于可穿戴传感数据识别用户日常行为方面发挥了重要作用，该技术可广泛应用于医疗、交通、安全监控等场景[19].

基于可穿戴设备的 HAR 问题被形式化为：给定一个包含有 k 个时间序列的集合 $S=\{S_0,\cdots,S_{k-1}\}$，其中，每个数据序列 S_i 采集自某个特定的被测量属性，测量的时间区间为 $I=[t_\alpha,t_\omega]$. 问题的目标是：给定一个测量数据集合 S 和一个个体活动类型标签集合(比如坐、行走等)，找出一个时间区间 I 的划分 $\langle I_0,\cdots,I_{r-1}\rangle$，使得每个时间子区间 I_j 对应到一种活动类型. HAR 问题中的时间子区间是连续的、非空的和不重叠的，即满足如下三个条件：(1)$\bigcup_{j=0}^{r-1}I_j=I$；(2)$\forall j\in\{0,\cdots,r-1\}$，有 $I_j\neq\varnothing$；(3)$\forall j,k\in\{0,\cdots,r-1\}$ 且 $j\neq k$，有 $I_j\bigcap I_k=\varnothing$. 显然，上述的定义假设个体活动不是并发的，即一个人不会同时坐和行走. 考虑到 HAR 问题无法保证可求解，并且属性个数与活动类型数目增加使得准确找到活动类型变化的时间点变得很困难，因此，一个松弛的 HAR 问题被形式化为：给定(1) m 个等长度且带有全部(或部分)标签信息的时间窗口集合 $W=\{W_0,\cdots W_{m-1}\}$，其中，每个时间窗口子集 W_i 包含一个采集自 k 个被测量属性的数据序列集合 $\{S_{i,0},\cdots,S_{i,k-1}\}$，以及(2)一个个体活动标签的集合 $A=\{a_0,\cdots,a_{n-1}\}$，问题目标是：找出一个从时间窗口集合到个体活动标签集合的映射函数 $f:W\to A$,使得对于任意的 $W_i\subset W$ ($i\in\{0,\cdots,m-1\}$)，识别结果 $f(W_i)$ 与 W_i 时间内的真实活动类型尽可能匹配. 因此，HAR 系统设计依赖于待识别的活动集合，不同的活动集合 A 对应着不同的 HAR 问题. 一般来讲，HAR 处理流程包括三个步骤(即数据采集、特征提取和学习与推断)和两个阶段(即训练和测试) [20]，如图 2 所示.

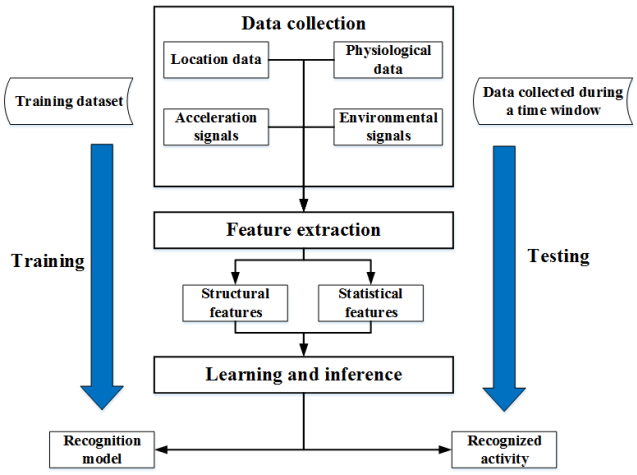

Fig. 2 Illustration of data flow for human activity recognition based on wearable sensors

图 2 基于可穿戴传感器的个体活动识别数据流图

值得注意的是，大多数 HAR 系统采用了有监督学习算法来训练行为识别模型，因为在一个完全没有样本标签信息的上下文中实现个体活动识别是非常困难的. 常见的有监督学习方法包括核方法、决策树、贝叶斯网络、K 近邻、神经网络、支持向量机、模糊逻辑、回归方法、马尔可夫模型、Boosting 级联等. 公开且权威的数据集能够有效地支撑 HAR 方法的设

计、实现与改进，比如：个人公开的数据集[21,22]、知名高校公开的数据集[23,24]以及活动识别挑战赛数据集[25]等.

1.4 面向行为分析的数据挖掘机制

当前，研究人员逐渐重视使用可穿戴设备来收集多种低层次的原始量化数据，然后利用智能处理方法挖掘更高层次的信息，例如行为特征提取与分析[26]、行为判别[27-29]、姿态识别[30]、用户兴趣检测[31]等. 因此，在可穿戴设备移动计算环境中，面向行为分析的数据挖掘机制是一个重点研究方向，在数据挖掘框架和个体数据挖掘机制等方面已经取得了一些研究成果. 值得说明的是，本文主要讨论可穿戴设备计算环境中的数据挖掘机制如何分析传感数据以及如何给人们隐私安全带来潜在威胁，而不涉及数据挖掘机制本身的安全和隐私问题，例如模型提取攻击和分类器参数泄漏.

1.4.1 分层数据挖掘框架

移动终端和可穿戴设备的飞速发展与大规模普及催生了海量的个体数据. 这些数据可能在传输通信过程中被分析、窃取，也可能被恶意攻击者利用数据挖掘技术发现隐藏的知识模式，例如用户习惯性活动、用户生理状况、移动轨迹等[32-36]. 传统数据挖掘系统中，中央数据处理系统(Data Processing System, DPS)负责采集所有的数据，随后加以分析以获得面向不同应用领域的知识模式. 然而，这种数据处理方式不适用于可穿戴计算场景，具体表现在如下两个方面：(1)可穿戴设备分布广泛，并且每一种类型的可穿戴传感器仅持续采集特定类型的数据，使得集中式数据采集过程变得困难；(2)大多数原始数据流相关度不大，DPS 需要耗费大量的计算资源来预处理数据以及存储空间来存储这些不相关数据. 为此，分层数据挖掘框架成为当前面向可穿戴设备的数据挖掘机制研究的主流.

文献[36]提出了一个统一框架 UniMiner 来实现可穿戴计算场景中的数据挖掘效益和代价之间的平衡. 在研究 OMM、CAROMM、PDM、CARDAP 等数据挖掘系统工作原理并分析各自优缺点的基础上，UniMiner 整合了可穿戴设备、资源受限环境、协同式数据处理系统和基于云的数据处理系统等来提供充足的计算资源. UniMiner 框架包括了三个层次：本地分析层(Local Analytics, LA)、协同分析层(Collaborative Analytics, CA)和基于云的分析层(Cloud-enabled Analytics, CLA)，如图 3 所示.

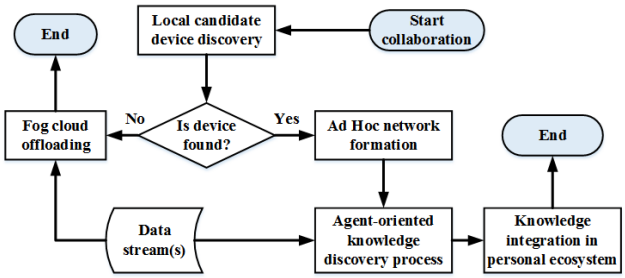

Fig. 4 Data processing flow of the collaborative analytics layer

图 4 协同分析层的数据处理流程

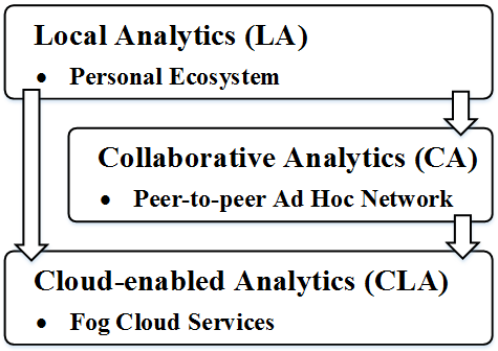

Fig. 3 Hierarchical architecture of UniMiner

图 3 UniMiner 分层架构

本地分析层包括如下四个功能模块:

(1)知识发现模块(KDM)：该模块实现数据预处理(比如降噪、降维、处理缺失数据)、数据挖掘算法库(比如聚类、分类、模式挖掘等算法)、临时数据存储(比如中间知识模式的存储)等功能.

(2)系统管理模块(SMM)：该模块更新计算资源信息(比如上下文信息和用户隐私设置)，其功能由自适应引擎、上下文管理、配置管理和资源监控等四个子模块构成.

(3)知识管理模块(KMM)：该模块实现本地知识模式的存储和集成，以及实时数据分析等功能.

(4)可视化模块(VIM)：该模块确保以最小资源需求展示集成后的知识模式和历史数据.

协同分析层的数据处理流程如图 4 所示，其中自适应引擎组件搜索局域内的备选设备以进行成对协作. 在获得各个设备内的资源列表后，自适应引擎组件确认资源可用性. 如果配对成功，主 Agent(部署在发起请求的设备)调度数据挖掘任务，候选设备完成知识发现任务并将结果发送给发起任务请求设备的自适应引擎组件；如果在规定时间内没有收到候选设备确认匹配的响应，那么发起任务请求设备的自适应引擎组件撤销协同分析任务，并重新指派任务给其他候选设备. 如果没有任何一个候选设备响应，那么发起任务请求设备的自适应引擎组件将调度或重定向数据流给基于云的分析层.

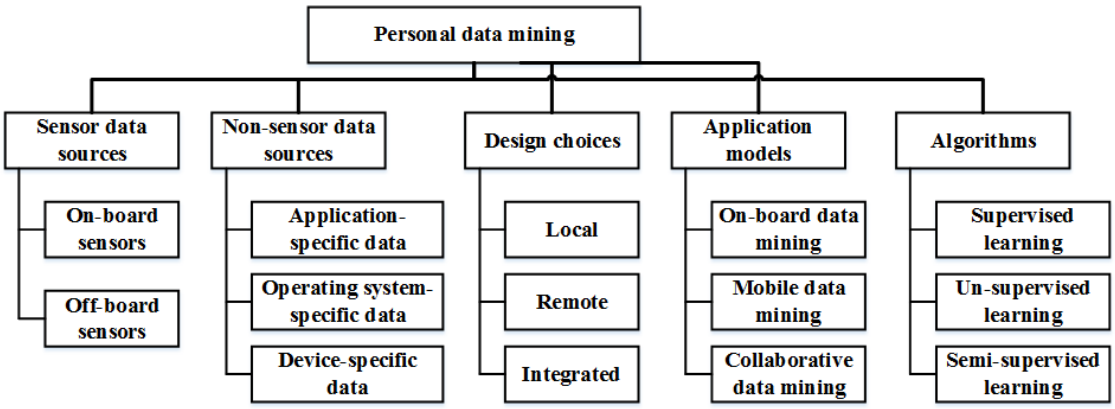

Fig. 5 Taxonomy of personal data mining mechanisms in resource-constrained environments

图 5 资源受限环境下的个体数据挖掘机制分类体系

基于云的分析层利用了雾云服务(Fog Cloud Services)进行数据分析，其中雾云服务特指那些靠近数据源端的云服务. 雾云技术最早由 Cisco 提出,它的架构包括三个层次：物联网层、接入层(比如 2G/3G/4G、LAN、WLAN)和靠近数据源的云端.

1.4.2 个体数据挖掘机制

在可穿戴计算场景中，个体数据挖掘是指利用数据挖掘技术来分析用户数据，从而满足某些特定的需求. 以可穿戴健康设备为例，对于设备拥有者来讲，他们希望可穿戴计算服务提供商借助个体数据挖掘技术来帮助其养成更为健康的生活方式；而对于攻击者来讲，他们更热衷于使用个体数据挖掘技术分析与受害目标相关的多源感知数据，进而挖掘其日常生活样式和健康状况，为发起其它类型的攻击(比如盗窃、垃圾健康类产品推介、欺诈等等)打基础. 近年来，与个体数据挖掘机制相关的研究工作呈现出了多元化趋势，具体来讲，这些研究重点可归并为五大类：基于不同的传感器数据源、基于不同的非传感器数据源、基于不同的设计策略、基于不同的应用模型以及基于不同的机器学习算法. 资源受限环境下的个体数据挖掘机制分类体系见图 5[35]. 在数据挖掘算法性能评价方面，权威数据集对于提出新型数据挖掘方法来讲具有重要的支持作用，比如 SPMF contextPasquier99[37,38]、UCI mushrooms 和 retail[39]等.

可以预见，基于多源感知数据的数据挖掘机制将仍然是热门研究方向之一. 此外，我们认为下一步的研究将更加注重多维度融合，例如，面向可穿戴计算应用的集成化、半监督移动数据挖掘方法.

2 面向可穿戴设备的数据安全与隐私保护技术

2.1 云辅助的隐私保护机制

在可穿戴计算中，数据采集过程通常发生在目标周边的传感器上，而数据汇聚过程则通常发生在第三方智能设备(比如能量受限的手持式移动设备)上. 由于可穿戴传感器和第三方智能设备是资源受限的，它们无法在本地存储实时采集的海量传感数据(比如数字、文本、图片)，也不能运行高能耗的计算任务. 为此，近年来大量的相关研究着重引入云计算来辅助完成计算密集型任务[40,41]，虽然面向可穿戴设备的隐私保护与云计算并不存在显式依赖性，但是云计算技术能够极大地便利可穿戴应用服务提供商完成复杂的、兼顾隐私安全的多源感知数据处理任务，进而增强可穿戴应用的隐私保护质量[42,43]. 近年来，云辅助的隐私保护机制重点研究面向可穿戴应用的隐私保护协议和可穿戴通信中的隐私安全保护两个方面的内容.

2.1.1 面向可穿戴应用的隐私保护协议

随着可穿戴设备大规模普及，可穿戴应用层出不穷，典型的例子有电子健康医务系统、智能家庭、智能健康运动等. 以电子健康医务系统为例，目标患者身上部署一些体征传感器，这些传感器实时采集个人健康体征数据，随后，这些体征数据被发送给健康医务云服务器. 为了确保敏感数据不被滥用，被授权的医生才能够访问数据，将其与云中的医疗模板进行类型相似度匹配以判断出患者身体状况，进而做出医疗诊断. 然而，将数据存储和计算处理过程从可穿戴设备迁移至不可信的第三方易于诱发许多隐私安全问题，代表性的有暴露身份隐私、泄露传输过程中的信息、公开位置信息、非法访问敏感数据、由恶意用户攻击或者误操作导致的可穿戴计算系统可用性降低等等[42]. 为了保护可穿戴应用中的隐私安全，研究者分别提出了隐私保护的动态文本挖掘与图片特征提取[41]、安全的数据访问与处理、误用行为检测[42]等方法与机制.

同样以电子健康医务系统为例，文献[42]指出加密存储健康数据以及使用认证技术防止非授权访问仅

仅是粗粒度的数据安全机制，进而提出了采用基于属性的加密方法来实现细粒度的数据安全. 而在误用检测方面，文献[42]首先讨论了严重影响电子健康医务系统性能的攻击样式. Sybil 攻击是该系统面临的一种较为典型的攻击类型. Sybil 攻击者使用大量伪造的别名或身份来欺骗受害者，进而影响其观念和偏好. Sybil 攻击者按照其能力从低到高可分为四个层次：(1)一般的 Sybil 攻击者(频繁修改别名来隐藏其真实身份)；(2)伪造通讯信息的 Sybil 攻击者(通讯记录无签名)；(3)与移动用户共谋的 Sybil 攻击者(通讯记录具有有效的签名)；(4)与云服务提供商共谋的 Sybil 攻击者(添加伪造的通讯记录或者修改/删除正常用户的通讯记录). 随后，文献[42]介绍了针对不同层次 Sybil 攻击的防御方法.

2.1.2 可穿戴通信中的隐私安全保护

在将任务外包给云端的过程中，如何保护个人隐私数据不被泄露成为了新的挑战性问题. 文献[40]探讨了无线可穿戴通信中的安全与隐私问题，特别是隐私保护的数据汇聚方法. 云辅助的无线可穿戴通信架构如图 6 所示，其中，可穿戴设备被部署在移动用户身上，持续地采集个体数据并将其安全地传输给云端；云端执行数据汇聚操作并将计算结果发送给授权的汇聚数据接收者；最后，汇聚数据接收者通过解密和恢复技术获得原始的数据汇聚结果.

Fig. 6 Architecture of cloud-assisted wireless wearable communications

图 6 云辅助的无线可穿戴通信架构

为了满足数据隐私、汇聚结果隐私、汇聚结果可验证以及高效等需求，隐私保护的数据汇聚方法通常使用如下三种实现技术：安全多方计算(Secure Multiparty Computation, SMC)、全同态加密(Fully Homomorphic Encryption, FHE)和单向陷门函数.

安全多方计算(SMC)要求多个参与方协同且隐私地计算一个函数 $\{y_1,\cdots,y_n\}=f(x_1,\cdots,x_n)$，其中，$x_i$ 和 y_i 分别表示参与方 i 的输入和对应于该参与方的函数输出. 对于任意的参与方 $i\in\{1,\cdots,n\}$，该参与方对应的输出 y_i 与所有的输入 x_i ($i=1,\cdots,n$)有关联，但是该参与方不知道任何关于 x_k 和 y_k ($k\in\{1,\cdots,n\}$ 且 $k\neq i$). 由于任意多项式时间复杂度函数都能够被表达成一个多项式规模大小的组合电路，因此 SMC 协议通过评价混淆电路来实现. SMC 的通信代价依赖于电路规模，而其计算开销依赖于输入线缆的数量. 特别地，在两个参与方的情况下，对于唯一知道最终计算结果的参与方，协议要求在它的每个输入线缆上执行一次状态迁移，并且在电路中的每个门电路上执行一次对称的加密/解密操作. 在多个参与方的情况下，SMC 协议将函数表达成一个二进制电路，它要求每一个参与方在开始阶段知道每个输入线缆状态. 此外，协议要求每一对参与方在每个乘法门上执行一次状态迁移. 值得注意的是，该协议要求多个参与方在初始化阶段协同地构造好每个门的混淆表. 当作出每对参与方之间存在一个隐私通信信道的假设之后，一个更一般化的 SMC 协议将目标函数表达成一个算术电路，而不仅限于二进制电路，其中组合电路中包括有加法门和乘法门. 与原有 SMC 协议相比，新的 SMC 协议不需要计算公钥操作，而仅执行轻量级的加法和乘法操作.

虽然研究人员为提高 SMC 效率做了许多工作，但是大规模电路、大量交互通信以及状态迁移使得 SMC 协议的通信复杂度和计算复杂度都比较高. 因此，SMC 协议无法适用于隐私保护的可穿戴通信. 为了克服 SMC 方法效率低的问题，可穿戴设备可以将数据外包给云服务器，从而将高复杂度的计算任务迁移到云端执行. 为了实现数据隐私和汇聚隐私，该方法要求云服务器在密文域中执行数据汇聚操作，其中，可穿戴设备在外包原始数据给云服务器之前对这些数据进行加密处理.

FHE 同时支持针对密文的加法和乘法操作，从而保护明文隐私[44]. FHE 方法的大致工作流程包括：(1)数据拥有者使用接收者的公钥加密数据序列；(2)云服务器在密文上进行加法和乘法操作，而只有被授权的接收者才拥有解密结果密文所需的密钥. 然而，对数据进行 FHE 操作违背了混合加密基本原则，即公钥加密通常被用于加密位数较少的对称(会话)密钥，而这些对称(会话)密钥被用于加密位数较长的数据. 此外，FHE 的实用面临着如下挑战：(1)大多数工作基于格中的多项式界这一难度的问题，并且明文需要被逐比特加密，从而导致 FHE 很难适用于可穿戴设备中海量数据被频繁采样和处理的场景；(2)外包计算验

证的安全挑战，其中，外包计算验证被用于向数据汇聚结果的接收方证明云计算结果的正确性；(3)外包计算验证的计算开销大，甚至超过了自己计算目标函数所需的计算开销.

由上述分析可知，SMC 和 FHE 的计算开销大，并且 FHE 方法违背了混合加密的基本原则. 为了解决这些问题，有研究者提出将单向陷门函数引入云辅助的可穿戴通信[41]. 根据应用场景不同，可穿戴设备可灵活地选择单向陷门函数以实现细粒度的数据访问授权. 典型的基于单向陷门函数的可穿戴通信机制有：基于任意单向陷门函数的加法同态隐私保护数据聚合机制、基于任意单向陷门函数的全同态隐私保护数据聚合机制和安全且高效的可验证外包计算机制.

2.2 隐私感知的个人信息发布机制

随着可穿戴设备的不断普及应用，人们能够很方便地分享其健康与生活状态信息. 例如，一些人分享自己的健康信息给他们的家人、朋友、医师、雇主、保险公司、研究人员等，以更好地改善其健康状态. 一般来讲，接收分享信息的人或团体被统称为信息接收者. 信息共享者可通过分享其个人信息以获得一定的效用(具体是指信息分享者通过分享个人信息所能够获得的好处). 然而，信息共享者需要权衡信息公开的程度与效用. 一方面，过多地分享个人信息能够获得更多收益，却增加了个人隐私信息被泄露的风险；另一方面，如果信息共享者分享的信息满足不了信息接收者的需求，那么其效用将减少. 与一般的个人敏感信息相比，可穿戴设备相关的个人敏感信息具有如下几个方面的差异：(1)从数据本身的特点来看，一般的个人敏感数据通常是与用户身份信息、爱好和习惯等相关的长期隐私数据，而可穿戴设备相关的个人敏感数据则一般是与个人日常生活相关的短期通知数据（例如日程安排和接收到的消息）以及与第三方应用交互相关的瞬时健康测量数据（例如心率测量数据和体型数据）和实时位置数据；(2)从敏感数据的采集时间方面来看，一般的个人敏感数据通常是被定期地（或周期性地）采集，而可穿戴设备相关的个人敏感数据则一般被实时且不间断地采集；(3)从敏感数据存储位置来看，一般的个人敏感数据通常被存储到永久存储介质（例如 U 盘、闪盘、磁盘、光盘等）上，而可穿戴设备相关的个人敏感数据被存储到与可穿戴设备相匹配的移动设备上；(4)从敏感数据使用者来看，一般的个人敏感数据通常由本人支配使用，而可穿戴设备相关的个人敏感数据还可被第三方应用开发者访问和使用. 下面的内容将从数据发布前和数据发布过程中这两个方面分别介绍隐私保护的数据发布方法.

2.2.1 数据发布前的隐私保护数据发布方法

为了保护敏感信息不被泄露，同时有效地保持数据在发布后的可用性，国内外学者提出了面向聚类的隐私保护数据发布方法[45,46]. 文献[46]提出了一种基于对等用户间数据聚合的隐私保护方案. 方案的基本思路是：用户 A 在提交数据之前，将数据分为N个分片，其中的M个分片分发给M个可信任的对等用户，本地仅上传剩余的$N-M$份数据分片. 通过这种方式，包含服务端在内的潜在不可信实体至多可以将 $N-M$ 份数据关联到用户 A，从而降低了基于上传和发布的数据进行身份推断的可能性. 针对被发布数据中可能存在的隐私泄露风险往往难以界定的问题，一种可行的解决途径是隐私保护者在数据发布之前对其进行扰动处理.该策略通过向采集的信息中加入预先设计的噪声信息来有效地隐藏与用户相关的真实数据，从而达到隐私保护的目标. 设计基于数据扰动的隐私保护方案时，隐私保护者需要选择合适的干扰噪声，充分权衡引入干扰噪声后数据的可用性和隐私保护收益. 文献[47]所提出方案的思路是：利用近似模型生成一个与真实的数据集特征相似的噪声模型，然后所有的设备利用该噪声模型扰动原数据以隐藏个人信息. 当数据汇总之后，隐私保护者执行聚合计算(包括求和、求均值等). 由于干扰噪声的分布特征已知，因此通过去除聚合结果中的噪声信号序列就可以得到真实的、可发布的聚合结果.

2.2.2 数据发布过程中的隐私保护数据发布方法

针对过度的数据分享将给人们带来了巨大的隐私信息泄露风险，文献[48]提出了一种隐私感知的个人信息分享架构 ShareBuddy，以在个人信息公开的程度与效用之间找到均衡点. 在 ShareBuddy 架构中，信息接收者请求个人信息，指定信息分享方在成功满足一个请求后所能获得的收益，并且支持向信息分享方发送一个关于信息分享风险的警报. 基于 ShareBuddy 架构的个人信息发布与接收流程如图 7 所示，其中信息分享方的 ShareBuddy 存储通过可穿戴设备采集的数据，辅助决策分享哪些数据、分享给谁等；信息接收者的 ShareBuddy 主要负责发送请求、接收和查看分享信息方发来的数据；ShareBuddy Web 服务允许信息采集应用的开发者注册其应用、允许信息接收者请求数据以及在信息分享方与信息接收者之间传输请求信息和数据信息. 该架构的优点是它能够帮助信息分享方明确发布个人信息的好处和风险，在获得收益和保护隐私两个目标上取得折衷. 此外，密码学加密技术被用于保护信息分享请求的隐私安全和被发布数据的隐私安全，使得请求消息和被分享的数据只能被合法的信息共享者和合法的信息接收者读取，从而

保护了个人信息发布全过程中的数据隐私.

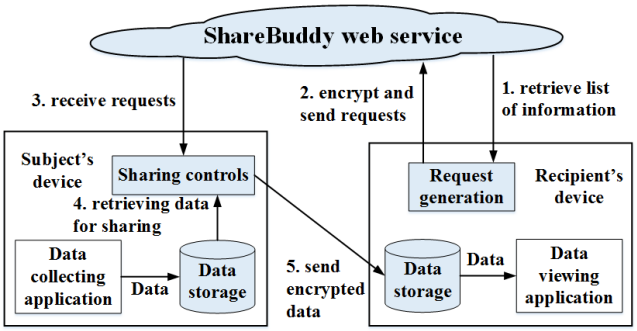

Fig. 7 Workflow of disclosing and receiving personal information based on the ShareBuddy architecture

图 7 基于 ShareBuddy 架构的个人信息发布与接收流程

2.3 基于访问控制的隐私保护机制

当前，传感器和无线传感网络已被广泛应用于多种应用场景，比如家庭和工业自动化、智能城市、电子医疗等等. 身体传感网络(Body Sensor Network, BSN)成为一种新兴的组网样式[49,50]. 一个 BSN 包括两类节点，即能力强的节点(Power Node)和微节点(Micro/Nano Node)，前者具有较强的计算能力并且资源约束较低，比如定制的信息接收节点；后者只具备有限的计算能力、存储空间、能量资源等，比如可穿戴设备和植入式设备.

近年来，针对 BSN 设计出合理的访问控制机制和隐私保护机制是一个热门的研究内容. 相关研究工作的分类见图 8.

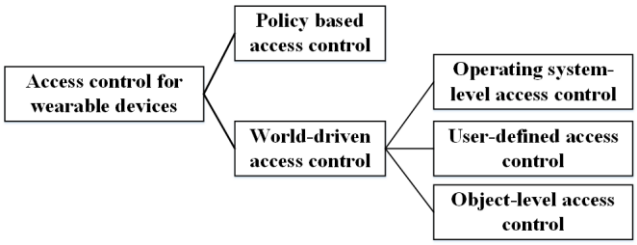

Fig. 8 Categories of access control mechanisms for wearable devices

图 8 可穿戴设备的控制访问机制分类

2.3.1 基于策略的访问控制机制

文献[51]以访问控制机制为研究重点，提出了一种基于策略的、跨平台的访问控制框架. 该框架基于标准的可扩展访问控制标记语言(eXtensible Access Control Markup Language, XACML)，为 BSN 资源和服务提供了一个细粒度访问控制机制. 一个 XACML 架构包括四个组件，即策略执行点(Policy Enforcement Point, PEP)、策略决策点(Policy Decision Point, PDP)、策略管理点(Policy Administration Point, PAP)和策略信息点(Policy Information Point, PIP)，分别执行访问控制、评价可用策略、创建并管理策略或策略集和提供属性值.

为了实现基于策略的访问控制框架，每个传感器遵循面向 Web 服务的设备轮廓(Devices Profile for Web Services, DPWS)规范，例如，一个温度传感节点被实现成一个 DPWS 设备，该设备托管一个与体温有关的服务并提供如下操作：(1)GetTemperature：返回目标当前体温；(2)TemperatureEvent：允许一个客户端医疗设备定制该服务、定期获得更新的体温信息以及在体温超过设定阈值时发出体温警告信息；(3)SetTemperatureThreshold：用于设置/更新体温警告阈值.类似地，每个传感节点的 XACML 组件也被表达为 DPWS 设备. 以温度传感节点为例，当某个医生试图访问体温信息时，首先发起一个 GetTemperature 请求；随后，体温监控设备自动地将该请求转发给 PEP 组件，进而 PEP 触发一个访问请求 AccessRequest 并将该访问请求发送给 PDP 组件；当 PDP 组件基于 PAP 组件中的策略规则和 PIP 组件中的属性值完成访问请求评价之后，它返回授权结果 PDPResponseEvent 给 PEP 组件；最后，访问控制决策结果被转发给体温监控设备，以最终决定该医生是否能够获得 GetTemperature 操作的结果. 此外，基于策略的访问控制框架使用安全协议保护交互的消息，比如传输层安全(Transport Layer Security, TLS)协议及其变种协议.

2.3.2 面向真实世界中持续感知的访问控制机制

目前，新兴的可穿戴设备(比如微软的 Kinect、谷歌的 Google Glass 和 Meta Space-Glasses 等)具备持续感知能力，这些设备的出现使得用户能够通过感知姿态完成操作输入以及通过感知声音完成指令下达. 然而，来自不可信应用的持续感知能力将会带来严重的隐私问题. 例如，当一个用户穿戴着 Google Glass 进入一个更衣室，就可能存在如下四种隐私问题：

(1)Word Lens 或者其它不可信的应用可能感知到了用户自身和周边人员的敏感信息；

(2)该用户可能在进入更衣室之前忘记关闭摄像头，使得 Google Glass 记录了周边人员的信息；

(3)该用户可能在更衣室的镜子面前忘记关闭摄像头，使得 Google Glass 记录了自身的信息并将其自动分享到社交媒体上；

(4)恶意用户可能使用 Google Glass 去记录其他人的信息.

在上述四种隐私问题中，前三种问题是不可信应用带来的隐私问题或者用户配置失误，而最后一种问题则是恶意用户有意侵犯他人隐私.

已有的一种隐私保护方法是在操作系统中设定好应用的权限. 目前，主流操作系统平台都默认拒绝

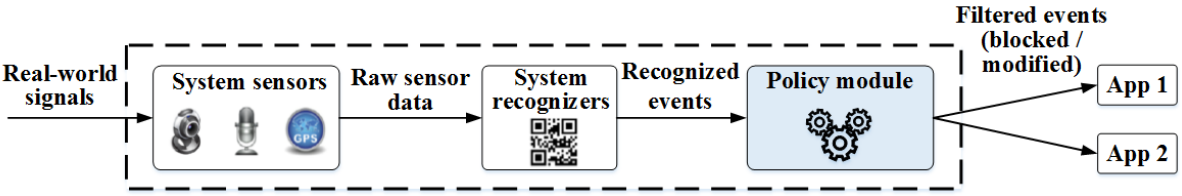

Fig. 9 World-driven access control framework

图 9 真实世界驱动的访问控制框架

不可信应用访问敏感资源，包括摄像头、GPS 等．在权限授权方面，不同操作系统的处理方式不尽相同：Android 和 Windows 8 系统在安装应用的时候确定访问权限；iOS 系统在访问敏感数据的时候提示确定访问权限．然而，这些方法无法适应持续感知和用户动态输入的场景．具体来讲，当应用程序不在敏感数据使用的上下文中时，用户难以确定应用需要什么权限以及为什么需要特定的权限；另一方面，在敏感数据使用过程中频繁地提示权限授权容易造成用户的“提示疲劳”，导致用户简单地点击“是”以使用敏感数据．

另一种隐私保护方法是用户驱动的访问控制机制，该机制将用户行为与应用权限授权相结合，以解决前一种方法的不足．然而，这种方法依赖于显式的用户与设备间交互，因此，它不能很好地应用于持续感知的场景．此外，对于接收用户输入(比如姿势、声音)的应用，该方法也需要摄像头或者麦克风持续工作．因此，该方法针对整个传感器流进行权限授权，是一种过于粗粒度的访问控制机制．

为了实现持续感知中的隐私保护，文献[52]重点关注不可信应用带来的隐私问题，提出了一个通用的、可扩展的访问控制框架，以保护多应用持续感知平台上的传感数据，如图 9 所示．特别地，该访问控制框架支持真实世界中的目标对象显式地指定访问控制策略，从而减轻了用户权限管理负担，并使得访问控制的粒度达到对象级别．

在真实世界驱动的访问控制框架中，作者提出了“护照”的概念[52]，其中一个护照指定了与某个目标对象相关的访问控制策略以及该对象如何被组织的编码方法(可选)．可穿戴设备操作系统中的一个可信策略模块检测目标对象护照、提取访问控制策略并将其动态地应用于移动应用中，以控制应用对敏感数据的访问．换句话说，用户自身不指定策略，而是依赖于可穿戴设备自动检测与配置真实世界中目标对象广播的访问策略．例如，一个运行了真实世界驱动的访问控制机制的 Google Glass 将检测一个更衣室对象通过蓝牙或者其它无线通信技术广播的“禁止摄像”的访问策略．随后，Google Glass 根据更衣室对象的策略自动地停止摄像．通过使用护照，真实世界驱动的访问控制框架能够在保护用户隐私不被不可信应用侵犯的同时减轻了用户显式管理访问控制策略的负担．此外，护照也可以帮助避免用户在无意识情况下分享自身隐私信息或者允许应用访问隐私信息．

在实用过程中，真实世界驱动的访问控制机制需要克服如下挑战：

(1)需要适应多种不同的访问策略通信机制，比如 QR 码、蓝牙或者目标识别等；

(2)识别护照和计算访问控制决策结果导致应用延迟；

(3)计算访问控制决策过程可能存在误报和漏报；

(4)由于移动、篡改或删除访问策略通信点所带来的新访问策略认证问题．

3 实例分析

近年来，可穿戴健康跟踪设备层次不穷，代表性的有：Basis B1 Band、Bowflex Boost、Fitbit Force、Fitbit Flex、Fitbit One、Fitbit Zip、Fitbug Orb、Garmin VivoFit、MIO Alpha BLE、Jawbone UP、Misfit Shine、Motorola MotoActv、Nike+ FuelBand SE、The Polar Loop 和 Withings Pulse．这些可穿戴设备跟踪的健康指标包括：燃烧的卡路里、心率、步数、睡眠节奏等．与过去具有相似功能的设备相比，新一代可穿戴健康跟踪设备支持绑定用户的在线社交网络帐号，实现实时采集和共享用户体征数据．此外，新一代可穿戴健康跟踪设备可借助高能效的短距无线通信技术与其它移动设备相互通信，易于融入规模尺度更大、架构更加复杂的网络，例如物联网(Internet of Things, IoT)．

由于在线社交网络在设计之初就侧重于开放与共享，因此它没有提供有针对性的用户隐私保护机制．当健康跟踪设备与社交网络集成之后，健康敏感数据的安全与隐私问题日益突出．另一方面，在可穿戴健康跟踪设备的设计与开发重点关注嵌入式传感器的测量精度，很少关心设备的安全与隐私问题．以倍受关注的 Fitbit 健康跟踪设备为案例，文献[47]分析了 Fitbit 设备、基站和 Web 服务器之间通信机制中的两个脆弱性，它们是：

(1)明文登录信息：用户发送给 Web 服务器的口令是明文传输的，并且口令以明文方式存储在日志文件中；

(2)明文 HTTP 数据处理：在同步健康数据到 Web 服务器时没有经过认证或者数据保护，即敏感健康数据以明文 HTTP 数据包的方式发送，导致恶意用户很容易捕获数据并获得健康跟踪设备的账号信息.

相应地，文献[53]提出了 FitLock 方法以应对 Fitbit 通信脆弱性，该方法由 BindUserTracker 和 UploadData 两个协议组成，用于可穿戴健康跟踪设备与 Web 服务器之间的安全交互过程中. BindUserTracker 协议被用来绑定可穿戴健康跟踪设备与用户；UploadData 协议被用来将健康敏感数据从健康跟踪设备上传至已通过认证的 Web 服务器上.

随后，文献[54]讨论了 FitLock 方法存在的一些隐私与安全问题，具体如下：

(1)可穿戴健康跟踪设备的标识不在加密范围内；

(2)FitLock 方法的两个协议都以明文方式广播健康跟踪设备的标识；

(3)恶意用户可以通过反复发送一个健康跟踪设备的标识给 Web 服务器，从而预取出一个响应集合. 这个响应集合可被用来实现重放攻击，伪造 Web 服务器的身份；

(4)由于可穿戴健康跟踪设备与 Web 服务器之间没有实行双向认证，因此，恶意用户能绑定一个被窃取的健康跟踪设备；

(5)在 UploadData 协议中，恶意用户可以通过反复阻塞从 Web 服务器发往健康跟踪设备的消息来发起解除同步攻击.

4 展望

在日常生活中，可穿戴设备持续地产生海量个体数据，从这些数据可以推断出身份、位置和健康情况等高价值信息. 医疗和健康类的应用使得可穿戴设备承载了越来越多的敏感数据[3]，这样也导致了越来越多的隐私泄露隐患. 另外，可穿戴设备非常轻便，易于携带，并且通常与随身携带的其它移动智能终端(如智能手机)组合使用，往往会给人造成不存在隐私泄露风险的错觉[6]. 目前，人们对于可穿戴设备的数据安全与隐私保护意识并不强，加剧了个体敏感信息被泄露的风险. 随着数据关联分析技术的不断发展，一些孤立的、看上去不敏感的个体数据一经关联，能帮助数据分析者推断出高层行为模式. 因此，可穿戴设备设计者和安全研究者必须考虑到每一部分数据的安全，可穿戴设备的隐私保护技术也亟需快速发展以满足需求. 目前研究者集中关注以下几个研究点，这也是面向可穿戴设备的数据安全隐私保护技术研究的未来研究热点：

(1)面向隐私保护的个体活动识别：可穿戴数据隐私保护和个体活动识别(包括用户状态识别)互为矛盾，又相互促进. 确保用户隐私不被泄露是敏感数据(如医疗数据等)得以安全发布的重要前提[3]. 随着数据挖掘技术(包含关联数据分析技术)的蓬勃发展，新型个体活动识别技术给现有隐私保护机制带来新挑战的同时，也反过来推动隐私保护技术不断向前发展[32-36]. 个别活动识别存在几个方面关键性的挑战：待测量属性的选择、可携带的数据获取系统、高效的特征提取与推断方法、真实条件下的数据收集、灵活便捷地支持新用户、基于移动设备的个体活动识别. 具体到可穿戴设备，基于多源可穿戴设备数据的个体活动识别技术着重研究如下八个方面的内容：权威的公开活动识别数据集、组合个体活动识别、并发个体活动识别、多个体属性分类、代价敏感的分类、基于群体的个别活动识别、未来个体活动预测和分类器灵活性研究[20].

(2)传统隐私保护技术的轻量化改造：可穿戴设备有限的计算和存储能力是制约隐私保护的客观原因，可穿戴设备内部资源有限性也使得开发者无法在设备上部署较为复杂的隐私安全机制[40]. 传统的隐私保护技术(例如加密认证、数字签名等)需要经过轻量化改造后才能应用到可穿戴设备上. 由于庞大且复杂的安全认证系统无法适用于可穿戴设备，因此面向可穿戴设备的安全认证技术将朝着轻量化和低时空代价方向发展，使得占用资源尽可能少.

(3)安全通信机制：受限于有限的存储和计算能力，可穿戴设备必然需要与云端设备、移动设备或其他可穿戴设备进行数据传输，这就对安全通信提出了很高的要求. 因为无法在设备内完成复杂的数据处理过程，可穿戴设备常常将采集到的数据直接(或者经过简单处理后)发送给云端完成数据处理与分析任务[40]. 为了保障可穿戴设备与云端服务器通信过程中的数据隐私，应当基于可穿戴设备特点，有针对性地设计和研究隐私保护的可穿戴通信机制. 在短距通信方面，Wi-Fi 和蓝牙技术是当前可穿戴设备之间、可穿戴设备与其它类型移动设备(例如手机和笔记本电脑)之间实现互联的主流技术. 然而，蓝牙和 Wi-Fi 等无线互联技术均易于遭受恶意攻击，进而给用户隐私泄露带来极大隐患[3]. 因此，面向可穿戴设备的安全短距通信技术有待下一步深入研究.

(4)低能耗的隐私保护技术：由于可穿戴设备能量受限，因此，隐私保护使用的各项安全认证技术、通

信传输技术都需要在确保隐私安全的前提下提高能效[20]. 如何节约可穿戴设备能耗是一个热门的研究课题. 值得预期的是隐私保护的可穿戴设备的数据处理和通信技术将会朝着低能耗方向不断演进.

(5)新型应用模式中的隐私保护：新型应用的出现使得可穿戴设备数据的产生和使用出现了新的模式. 例如移动群智感知(Mobile Crowd Sensing, MCS)是一种基于移动智能设备进行普适感知的新型传感网络范式[2]. 将可穿戴设备以传感节点的形式运用于 MCS 框架中，可以开展基于健康数据、运动数据乃至轨迹数据的应用，充分发掘以人群为单位的健康相关信息和移动模式. 然而，多样化、细粒度的数据收集和分析增加了用户隐私泄露的可能. 此外，相比于单个设备维度的数据集合，群组规模的数据汇聚和分析蕴含着更多规律和用户行为模式，为挖掘用户隐私提供了更多便利. 因此，如何针对新型应用模式进行可穿戴设备相关隐私信息的保护是一个值得深入探讨的研究问题.

(6)数据公开的原则和策略：出于社交、健康或者商家利益等需要，部分可穿戴设备数据可能会被公开. 如果恶意用户基于这些数据展开深层次分析，这将会给正常用户隐私带来异常严峻的挑战，因此更开放的信息发布和更严密的隐私保护是两个相互矛盾的目标. 如何在保障用户的数据公开需求以及保护数据隐私之间寻找到一个平衡点是一个非常值得研究的问题[42]，有关数据公开的原则和策略的研究仍待深入.

(7)针对可穿戴设备的攻击模型或模式：近几年来，与可穿戴设备隐私安全相关的事件时常出现，比如被动监控、远程命令执行、可穿戴设备任意绑定. 然而，目前极少有针对可穿戴设备的攻击模型和模式相关工作. 因此，如何建模针对可穿戴设备的攻击行为是一个紧迫的研究课题，有待下一步专门研究.

(8)法律伦理：技术是保护用户隐私的手段，而法律、道德和伦理则是保护用户的准绳. 可穿戴设备的广泛使用带动了相关技术的发展，但是法律伦理建设却没有跟上这一新生事物的发展. 例如，虽然某人购买了可穿戴设备，但是其个人数据的使用和存储却并未完全受其控制. 例如，Fitbit 不赋予用户数据控制权限，即未经用户许可而把用户的所有数据上传到公司的私有云上. 有没有可能使可穿戴设备成为非资源受限的设备，或部分特别敏感的数据在本地处理不上传，通过加强用户的数据控制权限，使用户成为可穿戴设备的“真正主人”. 这是一个特别有趣的研究话题，也需要围绕可穿戴设备的法律、道德和伦理的逐步完善来共同实现这个目标.

参 考 文 献

[1] He D, Chan S, Guizani M. User privacy and data trustworthiness in mobile crowd sensing [J]. IEEE Wireless Communications, 2015, 22(1): 28-34

[2] Hu X, Liu Q, Zhu C, Leung VCM, Chu THS, Chan HCB. A mobile crowdsensing system enhanced by cloud-based social networking services[C]//Proc of the 1st International Workshop on Middleware for Cloud-enabled Sensing (MCS'13). Beijing: ACM, 2013: 3:1-3:6

[3] Ameen MA, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications[J]. Journal of Medical Systems, 2012, 36(1): 93-101

[4] Latre B, Braem B, Moerman I, Blondia C, Demeester P. A survey on wireless body area networks[J]. Wireless Networks, 2011, 17(1): 1-18

[5] Hoyle R, Templeman R, Armes S, Anthony D, Crandall D, Kapadia A. Privacy behaviors of lifeloggers using wearable cameras[C]//Proc of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'14). Seattle: ACM, 2014: 571-582

[6] Yan T, Lu Y, Zhang N. Privacy disclosure from wearable devices[C]//Proc of the 2015 MobiHoc Workshop on Privacy-Aware Mobile Computing (PAMCO'15). Hangzhou: ACM, 2015: 13-18

[7] Peng H, Chen H, Zhang X-Y, Fan Y-J, Li C-P, Li D-Y. Location privacy preservation in wireless sensor networks[J]. Journal of Software, 2015, 26(3): 617-639(in Chinese)
(彭辉, 陈红, 张晓莹, 范永健, 李翠平, 李德英. 无线传感网络位置隐私保护技术[J]. 软件学报, 2015, 26(3): 617-639)

[8] Bai E, Zhu J. TinySBSec-The new lightweight WSN link-layer encryption algorithm[J]. Journal of Harbin Engineering University, 2014, 35(2): 250-255(in Chinese)
(白恩健, 朱俊杰. TinySBSec-新型轻量级 WSN 链路层加密算法[J]. 哈尔滨工程大学学报,2014,35(2):250-255)

[9] Lin H, Bai D, Cai Z, Liu Y. A packet coding data encryption algorithm for wireless sensor networks[J]. Journal of Southeast University (Natural Science Edition), 2012, 42(S1): 112-116(in Chinese)
(林海峰, 白荻, 蔡正宇, 刘云飞. 一种无线传感器网络的数据包编码加密算法设计[J]. 东南大学学报(自然科学版), 2012, 42(S1): 112-116)

[10] Yang G, Wang A-Q, Chen Z-Y, Xu J, Wang H-Y. An energy-saving privacy-preserving data aggregation algorithm[J]. Chinese Journal of Computers, 2011, 34(5): 792-800(in Chinese)
(杨庚, 王安琪, 陈正宇, 许建, 王海勇. 一种低耗能的数据融合隐私保护算法[J]. 计算机学报, 2011, 34(5): 792-800)

[11] Sweeney L. K-anonymity: A model for protecting privacy[J]. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10(5): 557-570

[12] Machanavajjhala A, Gehrke J, Kifer D, Venkitasubramaniam M. L-diversity: Privacy beyond k-anonymity[J]. ACM Transactions on Knowledge Discovery from Data, 2007, 1(1): Article 3, 52 pages

[13] Li M, Li T, Venkatasubramanian S. T-closeness: Privacy beyond

k-anonymity and l-diversity[C]//Proc of the 23rd International Conference on Data Engineering. Istanbul: IEEE, 2007: 106-115

[14] Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: A comprehensive survey[J]. Journal of Biomedical Informatics, 2015, 55: 272-289

[15] Das AK, Pathak PH, Chuah C-N, Mohapatra P. Uncovering privacy leakage in BLE network traffic of wearable fitness trackers[C]//Proc of the 17th International Workshop on Mobile Computing Systems and Applications (HotMobile'16). ACM, 2016: 99-104

[16] Li H, Wu J, Gao Y, Shi Y. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective[J]. International Journal of Medical Informatics, 2016, 88: 8-17

[17] Li M, Lou W, Ren K. Data security and privacy in wireless body area networks[J]. IEEE Wireless Communications, 2010, 17(1): 51-58

[18] Parkka J, Ermes M, Korpipaa P, Mantyjarvi J, Peltola J, Korhonen I. Activity classification using realistic data from wearable sensors[J]. IEEE Transactions on Information Technology in Biomedicine, 2006, 10(1): 119-128

[19] Yuan L, Liu Q, Lu M, Zhu C, Zhou S, Yin J. A Highly Efficient Human Activity Classification Method Using Mobile Data from Wearable Sensors[J]. International Journal of Sensor Networks, 2016(In Press)

[20] Lara OD, Labrador MA. A survey on human activity recognition using wearable sensors[J]. IEEE Communications Surveys & Tutorials, 2013, 15(3): 1192-1209

[21] Datasets for Human Activity Recognition from Tim Van Kasteren's Website[OL]. [2016-10-17] https://sites.google.com/site/tim0306/datasets

[22] Datasets for Human Activity Recognition from Tanzeem Choudhury's Website[OL]. [2016-10-17] http://www.cs.dartmouth.edu/~tanzeem/teaching/CS188-Fall08/dataset.html

[23] Datasets for Human Activity Recognition from MIT Media Lab[OL]. [2016-10-17] http://architecture.mit.edu/house n/data/PlaceLab/PlaceLab.htm

[24] Datasets for Human Activity Recognition from ETH's Wearable Computing Lab[OL]. [2016-10-17] http://www.wearable.ethz.ch/resources/Dataset

[25] 2011 Activity Recognition Challenge[OL]. [2016-10-17] http://www.oportunity-project.eu/challenge

[26] Bellos C C, Papadopoulos A, Rosso R, Fotiadis D I. Extraction and analysis of features acquired by wearable sensors network[C]//Proc of the 10th IEEE Conference on Information Technology and Applications in Biomedicine. IEEE, 2010

[27] Awais M, Palmerini L, Chiari L. Physical activity classification using body-worn inertial sensors in a multi-sensor setup[C]//Proc of the 2nd IEEE International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI). IEEE, 2016

[28] Liu X, Liu L, Simske S J, Liu J. Human daily activity recognition for healthcare using wearable and visual sensing data[C]//Proc of the 2016 IEEE Conference on Healthcare Informatics (ICHI). IEEE, 2016

[29] Gomes J B, Krishnaswamy S, Gaber M M, Sousa P, Menasalvas E. Mobile activity recognition using ubiquitous data stream mining[C]//Proc of the DaWaK 2012, LNCS 7448. Springer-Verlag Berlin Heidelberg, 2012: 130-141

[30] Iyer D, Mohammad F, Guo Y, Safadi E A, Smiley B J, Liang Z, Jain N K. Generalized hand gesture recognition for wearable devices in IoT: Application and implementation challenges[C]//Proc of the MLDM 2016, LNAI 9729. Springer International Publishing Switzerland, 2016: 346-355

[31] Englebienne G, Hung H. Mining for motivation: Using a single wearable accelerometer to detect people's interests[C]//Proc of the IMMPD 2012. ACM, 2012: 23-26

[32] Candas JLC, Pelaez V, Lopez G, Femandez MA, Alvarez E, Diaz G. An automatic data mining method to detect abnormal human behaviour using physical activity measurements[J]. Pervasive and Mobile Computing, 2014, 15: 228-241

[33] Banaee H, Ahmed MU, Loutfi A. Data mining for wearable sensors in health monitoring systems: A review of recent trends and challenges[J]. Sensors, 2013, 13(12): 17472-17500

[34] Zhao Q-L, Jiang Y-H, Lu Y-T. Ensemble model and algorithm with recalling and forgetting mechanism for data stream mining[J]. Journal of Software, 2015, 26(10): 2567-2580(in Chinese)
(赵强利, 蒋艳凰, 卢宇彤. 具有回忆和遗忘机制的数据流挖掘模型与算法[J]. 软件学报, 2015, 26(10): 2567-2580)

[35] Ur Rehman MH, Liew CS, Wah TY, Shuja J, Daghighi B. Mining personal data using smartphones and wearable devices: A survey[J]. Sensors, 2015, 15(2): 4430-4469

[36] Ur Rehman MH, Liew CS, Wah TY. UniMiner: Towards a unified framework for data mining[C]//Proc of the 2014 4th World Congress on Information and Communication Technologies (WICT'14). Bandar Hilir: IEEE, 2014: 134-139

[37] Fournier-Viger P. Spmf: A sequential pattern mining framework[OL]. [2016-10-17] http://www.philippe-fournier-viger.com/spmf

[38] Fournier-Viger P, Gomariz A, Gueniche T, Soltani A, Wu C-W, Tseng VS. SPMF: A Java open-source pattern mining library[J]. The Journal of Machine Learning Research, 2014, 15(1): 3389-3393

[39] Blake C, Merz CJ. {UCI} repository of machine learning databases[OL]. [2016-10-17] http://archive.ics.uci.edu.ml/

[40] Zhou J, Cao Z, Dong X, Lin X. Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions[J]. IEEE Wireless Communications, 2015, 22(2): 136-144

[41] Zhou J, Cao Z, Dong X, Lin X. PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems[J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 9(7): 1332-1344

[42] Zhang K, Yang K, Liang X, Su Z, Shen X (Sherman), Luo HL. Security and Privacy for Mobile Healthcare Networks: From a Quality of Protection Perspective[J]. IEEE Wireless Communications, 2015, 22(4): 104-112

[43] Liu W, Liu H, Wan Y, Kong H, Ning H. The yoking-proof-based authentication protocol for cloud-assisted wearable devices[J]. Personal and Ubiquitous Computing, 2016, 20: 469-479

[44] Preuveneers D, Joosen W. Privacy-enabled remote health monitoring applications for resource constrained wearable devices[C]//Proc of the 31st Annual ACM Symposium on Applied Computing (SAC'16). ACM, 2016: 119-124

[45] Chong Z, Ni W, Liu T, Zhang Y. A privacy-preserving data publishing algorithm for clustering application[J]. Journal of Computer Research and Development, 2010, 47(12): 2083-2089(in Chinese)
(崇志宏, 倪巍伟, 刘腾腾, 张勇. 一种面向聚类的隐私保护数据发布方法[J]. 计算机研究与发展, 2010, 47(12): 2083-2089)

[46] Shi J, Zhang R, Liu Y, Zhang Y. PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems[C]//Proc of the 29th IEEE International Conference on Computer Communications (INFOCOM). IEEE, 2010: 1–9

[47] Ganti RK, Pham N, Tsai Y-E, Abdelzaher TF. PoolView: Stream privacy for grassroots participatory sensing[C]//Proc of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys). ACM, 2008: 281–294

[48] Prasad A, Liang X, Kotz D. Poster: Balancing disclosure and utility of personal information[C]//Proc of the 12th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'14). Bretton Woods: ACM, 2014: 380-381

[49] Li H, Tan J. An ultra-low-power medium access control protocol for body sensor network[C]//Proc of the 27th Annual International Conference of the Engineering in Medicine and Biology Society (EMBS'05). Shanghai: IEEE, 2005: 2451-2454

[50] Lin C, Wang P, Song H, Zhou Y, Liu Q, Wu G. A differential privacy protection scheme for sensitive big data in body sensor networks[J]. Annals of Telecommunications, 2016, 71: 465-475

[51] Manifavas C, Fysarakis K, Rantos K, Kagiambakis K, and Papaefstathiou I. Policy-based access control for body sensor networks[C]//Proc of WISTP 2014, LNCS 8501. Springer Berlin Heidelberg, 2014: 150-159

[52] Roesner F, Molnar D, Moshchuk A, Kohno T, Wang HJ. World-Driven Access Control for Continuous Sensing[C]//Proc of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS'14). Scottsdale: ACM, 2014: 1169-1181

[53] Rahman M, Carbunar B, Banik M. Fit and vulnerable: Attacks and defenses for a health monitoring device[C]//Proc of the 34th IEEE Symposium on Security & Privacy (IEEE S&P'13). San Francisco: IEEE, 2014

[54] Zhou W, Piramuthu S. Security/Privacy of Wearable Fitness Tracking IoT Devices[C]//Proc of the 9th Iberian Conference on Information Systems and Technologies (CISTI'14). IEEE Computer Society, 2014

Liu Qiang, born in 1986. PhD, Assistant Professor. Member of China Computer Federation. His main research interests include 5G network, Internet of Things, wireless network security, and machine learning. (qiangliu06@nudt.edu.cn)

Li Tong, born in 1992. MS. His main research interests include network security and data security. (18739965789@163.com)

Yu Yang, born in 1992. BS. Her main research interests include big data and information security. (yuyang_nudt@163.com)

Cai Zhiping, born in 1975. PhD, Professor. Senior Member of China Computer Federation. His main research interests include network security and big data. (zpcai@nudt.edu.cn)

Zhou Tongqing, born in 1991. PhD candidate. His main research interests include network measurement and mobile crowdsourcing. (zhoutongqing@nudt.edu.cn)