传感云安全研究进展

王田[1]，李洋[1]，贾维嘉[2,3]，王国军[4]，彭绍亮[5]

（1. 华侨大学计算机科学与技术学院，福建 厦门 361021；2. 澳门大学数据科学中心，澳门 999078；
3. 上海交通大学电子信息与电气工程学院，上海 200240；4. 广州大学计算机科学与教育软件学院，广东 广州 510006；
5. 国防科技大学计算机学院，湖南 长沙 410073）

摘 要：通过调研大量的国内外传感云安全的相关文献发现，现有的传感云系统存在一系列严重的安全问题，如不同服务提供商的信誉问题、物理节点耦合漏洞、数据权限管理漏洞等，严重地阻碍了传感云系统的进一步发展。分析了传感云系统存在的安全问题，对比了现有的传感云安全技术，讨论总结了不同种类解决方案的优缺点，提出了未来传感云发展面临的安全挑战。最后，设计了基于雾计算框架下传感云安全的实现方案，为传感云的安全研究带来新的思路。

关键词：云计算；无线传感网；传感云；安全；雾计算

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018035

Research progress of sensor-cloud security

WANG Tian[1], LI Yang[1], JIA Weijia[2,3], WANG Guojun[4], PENG Shaoliang[5]

1. Department of Computer Science and Technology, Huaqiao University, Xiamen 361021, China
2. Data Science Center, University of Macau, Macao 999078, China
3. Department of Electronic Information and Electrical Engineering College, Shanghai Jiaotong University, Shanghai 200240, China
4. Department of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China
5. Department of Computer, National University of Defense Technology, Changsha 410073, China

Abstract: Through consulting lots of domestic and international literatures about sensor-cloud security, a series of security problems are found, such as reputation problem of service provider, the coupling problem of physical nodes, the leak of authority management, et al, which seriously hinders the further development of sensor-cloud. The secure problems occurring in sensor-cloud were analyzed, the current secure technologies were contrasted , similarities and differences of various types solutions were discussed and summarized. After that, several future challenges of sensor-cloud security were concluded. Finally, a fog-based structure was proposed to solve the security problems, which would bring new ideas to the sensor-cloud security research.

Key words: cloud computing, wireless sensor network, sensor-cloud, security, fog computing

1 引言

近年来，随着无线传感器网络（WSN, wireless sensor network）的发展和云计算的广泛应用，传感云（sensor-cloud）的诞生成为物联网发展的必然趋势。传感云由无线传感器网络和云计算组合而成，

收稿日期：2017-01-08；**修回日期**：2017-12-02

通信作者：王田，cs_tianwang@163.com

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2015CB352401）；国家自然科学基金资助项目（No.61772148, No.61672441, No.U1405254）；华侨大学研究生科研创新培育基金资助项目（No.1511414005）

Foundation Items: The National Basic Research Program of China (973 Program) (No.2015CB352401), The National Natural Science Foundation of China (No.61772148, No.61672441, No.U1405254), The Foster Project for Graduate Student in Research and Innovation of Huaqiao University (No.1511414005)

不仅继承了 WSN 无处不在的物理感知能力，还具有云计算强大的计算和存储能力，因此其应用领域也更加多样广泛。然而，安全问题是当前传感云系统面临的关键问题。一方面，网络信息技术的快速发展，为不法分子提供了良好的生存环境；另一方面，传感云体系特性如物理层传感器易获取、物理通信暴露、中间层虚拟化、数据远程外部存储等，使传感云系统存在不同的类型的安全漏洞，加重保护难度，因此，对传感云安全研究是极其必要的。

本文首先介绍了传感云的概念及实现框架，并强调了传感云安全研究的必要性。其次，根据传感云运行过程中数据动态，分析了传感云中存在的安全问题和 5 类安全保护技术。接着，对比了目前传感云的安全相关研究，从工业传感云平台安全机制到学术传感云安全文献，并总结了未来传感云安全的研究方向。最后，结合目前新兴的雾计算概念，为解决传感云安全问题提供了新思路。

1.1 传感云体系结构

传感云是传感器网络和云计算结合的产物[1]。无线传感器网络被广泛地应用在各个领域，如民用、国防军事、环境监测和建筑体监测等[2~5]，由于其在计算、存储、能量等诸多方面的限制，如何有效管理大规模无线传感器网络以充分发挥性能是一个亟待解决的问题。云计算的出现和发展为传感云的诞生提供了有利条件。云计算不仅可以满足传感器网络在数据处理和存储等方面的需求[6,7]，而且拓展了传感器网络的应用空间。在传感云系统中，传感网在底层收集用户需要的数据，并上传到云端，云服务器对数据进行加工处理并提供给用户。传感层对用户而言是透明的，用户不需要知道数据从何而来，只要按需获取云平台提供的服务即可。总之，传感云继承了云计算的运作模式，它将传感器网络与云计算进行整合，共享两者的资源，为用户提供远程的、高时效的按需服务。

文献[6]提出了一种抽象传感云的体系结构，如图 1 所示，它从下往上依次包含物理传感层、虚拟传感层和用户层。物理传感层由传感器节点组成，主要负责收集数据并与上层云端对接。在此层中，每个传感器节点有各自的控制与数据收集机制，不同的应用中的传感器节点具有不同的功能。例如，森林监测中的传感器节点只用于监测温度、湿度等必要信息；而目标跟踪中的传感器节点则要求实时返回目标的地理位置、移动轨迹等信息。虚拟传感层由虚拟传感器节点和云服务器组成，主要负责数据处理和对物理节点层调度管理，同时，虚拟传感层可为用户提供可视的、便捷的、安全的服务。由此实现物理节点对用户的透明化，用户不需要担心传感节点的具体位置和实时状态[8]。最上层为用户层，不同的用户可以通过虚拟传感层访问传感层收集到的数据。由于资源共享于云端，当用户获得相应的权限，便可访问其他用户资源。用户层面向用户提供一些远程需求服务并兼容不同的平台系统，如某些用户向传感云请求服务，这些服务可能来自不同的网络（3G、4G、Wi-Fi）、不同的终端（手机、平板、电脑）或不同的操作系统[9]（Windows、Linux、Mac）。

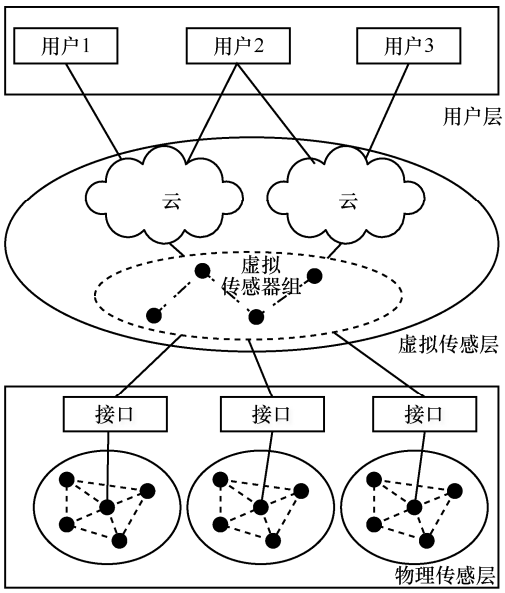
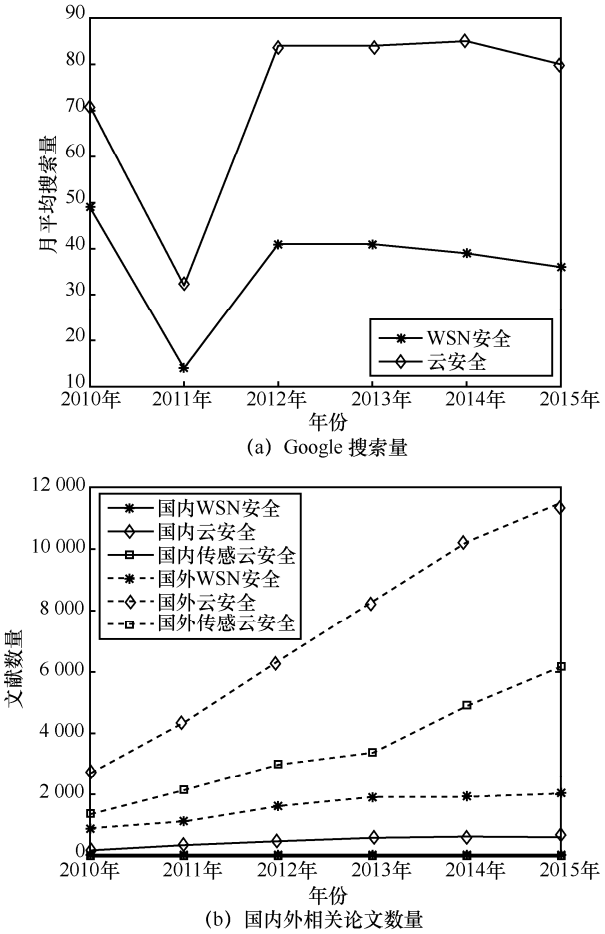


图 1 传感云体系结构

1.2 国内外传感云研究现状

本文通过对传感云及其安全问题的大量调研发现，传感云目前处于发展起步阶段，仅有少量国外文献进行过研究，国内相关研究则较少，关于传感云安全的研究更少。图 2(a)为近年来 Google 上有关传感网安全和云计算安全的搜索量趋势。从图 2(a)中可以看到，在 2011 年，两者的搜索热度有所下滑，但在 2012 年~2015 年，两者已经恢复并保持了较高的关注热度。图 2(b)为国内外已发表的相关文献数量趋势，其中，实线为国内科技期刊数据库检索的文献趋势，虚线为 Google 学术检索的文献趋势。从图 2(b)中可以看出，有关安全的研究论文数量均处于逐步上升的趋势，特别是国外关于“传感

云安全”的科研论文量（对应的传感云安全曲线），近年来保持了较快的增长速度。此外，从国内外文献数量对比可知，目前国内相关安全的文献相比于国外少了很多，特别是在“传感云安全”研究方向，其论文数量更少。



(a) Google 搜索量

(b) 国内外相关论文数量

图 2　WSN 与云计算安全研究趋势

在此背景下，本文梳理了传感云中存在的安全威胁，整理了传感云安全的研究现状，探讨了传感云系统安全应有的需求，对目前已有的方法分类分析，并展望了未来的研究方向和提出了基于雾计算框架的传感云安全新思路。

1.3　传感云应用背景

1.3.1　智能医疗领域

在智能医疗应用中[10]，人体健康数据，如体温、血压、脉搏及医疗图像等数据被不同种类的传感器实时监测并通过网关上传到云端，远程的医务人员通过从云服务器获取数据来诊断和治疗病人。一方面，健康信息需要被周期性地采集，记录相关数据的最大值、最小值或平均值，并将其与正常数值进行比较。另一方面，对于有相同疾病症状的病人，则需要收集来自同一地理区域，不同独立个体的健康数据，然后通过大量复杂的统计计算和多项式分析，如人口方差、欧几里得距离、样本偏差等，对其特征和病原细菌的进化状态进行学习。这种情况下，传统的无线传感网络则无法满足其大数据量的存储和计算的要求，因此，将数据传给云服务器存储和协助处理可以满足应用的需要。

1.3.2　车载网

车载网则是利用定位设备来提供基于位置的增值服务[11]。当车载网用户接近某一特定位置并按照喜好和需要请求附近餐厅、影院、商城等服务信息时，传统的传感网络无法长时间执行复杂的数据匹配算法，而基于定位的云服务器则可快速根据用户搜索标准比较附近商家的信息，并将合适的范围结果返回给用户。

1.3.3　智能电网

在智能电网应用中[12]，由于智能仪表在存储和计算能力的限制，智能电网则需要借助云服务器的存储和计算能力，利用外部计算确定区域是否处于用电高峰期（总用电量高于用电门限），或从空间和时间的角度聚合和分析用户的实时用电量，对应每隔一个周期动态地给用户充电。

1.4　传感云安全必要性

随着网络基础设施的完善、技术的提升，传感云系统被广泛应用于各个领域，不仅用户需求呈现多样化，对安全的要求也越来越高。传感云系统虽然具备传感网和云计算的强大能力，但是同样面临着两者自身存在的安全问题，甚至衍生出新的安全问题。上述 3 个典型的传感云应用，虽然为用户提供了极大的便利，但同时也给用户带来了一定的安全威胁。在智能医疗领域，病人的病例信息存储在外部云服务器中，当云服务器被攻击，病人的医疗信息则会被泄露。在车载网应用中，云服务器虽然提供了便捷的信息服务，但是会将用户的位置及个人喜好暴露给服务提供商；提供商可对数据进行挖掘和商业开发利用。在智能电网应用中，用户实时用电量暴露了用户生活习惯，这类数据如果被恶意窃取会对用户造成极大的安全隐患，例如，小偷了解用户生活习惯，对住户进行蹲点偷盗。因此，无论是哪类传感云安全威胁，都会给用户造成极大困扰，有的甚至威胁到用户自身的安全。传感云安全问题不可忽视且亟待解决。

2 传感云安全问题

本文给出了基于数据分类的传感云安全问题及传感网和云计算结合衍生出的新的安全问题，即虚拟化安全问题。

2.1 基于数据分类的安全问题

本节根据传感云中数据的流向将传感云安全问题分为4个阶段：数据产生阶段、数据传输阶段、数据管理阶段和数据服务阶段。

文献[13]提出了一个详细的传感云实现框架，如图3所示。在数据产生阶段，物理层通过传感器节点获取感知数据。在数据传输阶段，物理层内部将数据汇总到基站，然后基站将感知数据上传到云端。在数据管理阶段，云服务器对数据处理和存储。最后在数据服务阶段，数据通过虚拟传感层可视化地将数据提供给用户。接下来将分条阐述每个阶段的安全问题。

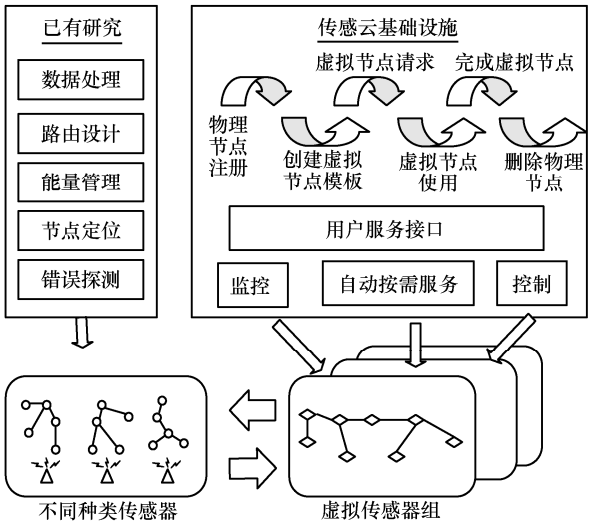


图3 传感云实现框架

2.1.1 数据产生阶段

传感云系统数据由传感器节点感知而来，传感器节点的工作环境特性导致传感云系统存在物理安全问题[14]。

由于传感云底层网络分布在无人看管的环境中，物理节点暴露在外面，极易被捕获和破坏，这为攻击者提供了便利的物理攻击条件。传感云中典型的物理攻击包括物理干涉、感知节点捕获、伪设备攻击等。物理干涉指攻击者故意干扰物理设备运行，如断电、重启等，导致设备无法正常运行[15]。物理威胁造成认证密钥、通信密钥等身份认证防护措施失效。伪设备攻击则是攻击者获取认证密钥后放置可进行身份认证的攻击节点，窃取机密数据或干扰正常节点通信。这些攻击对底层感知数据的完整性、可用性有着致命的破坏，且对数据感知之后的阶段也有着不可忽视的影响。

2.1.2 数据传输阶段

传感云数据传输有2个阶段：节点间数据的传输和基站与云端的传输，这2个阶段都面临着通信安全问题[16,17]。

通信安全可以防止数据在上传过程被监听和泄露，保护数据不被篡改或破坏。传感云中通信安全威胁既存在于传感网底层点对点通信，也存在于基站与云端的无线或有线通信。典型的攻击有阻塞攻击、时序攻击、转发攻击和路由攻击。阻塞攻击主要是恶意设备频繁广播信号，占用通信信道且增加了数据传播冲突的概率。在时序攻击中，攻击者通过分析加解密算法来获取密钥，并预测获取所有密钥的时间和解密数据分组需要的密钥数量。转发攻击主要发生在认证阶段，破坏证书的有效性。路由攻击则是攻击者恶意地制造路由环，导致有效数据无法正常传输到基站。

2.1.3 数据管理阶段

当数据上传到云端后，数据的管理安全存在3类问题：敏感数据定义[18]、数据共享安全[19]、数据存储安全[20]。

1) 敏感数据定义

传感云应用过程中，数据的种类繁多，其机密性程度也有所差异。数据的来源不同、产生时间不同、地点不同等因素均会影响数据的机密性。例如，当一个定位传感器监测到特定对象的移动轨迹时，则被当作敏感数据，而普通监测数据则会被一起上传，加重系统的处理负担，但也存在所有的监测数据都是高度敏感的，如个人医疗监测设备产生的生理数据。因此，传感云系统如何划分敏感数据、潜在敏感数据及普通数据影响了数据的机密性安全。另一方面，为了减少系统负担或提供准确的服务，具有相关性的数据会被组合存储，那么对于组合后的数据也存在敏感定义的问题。

2) 数据共享安全

传感云为多用户提供了一个高效的、低成本的、可扩展性强的资源共享平台，但同时也给安全带来了巨大挑战。共享系统一方面为数据安全风险的快速延伸提供了便利条件，另一方面多用户共享

的特征为恶意用户攻击其他用户或自私用户恶意抢占资源提供了机会，例如，常见的安全威胁有：侧信道攻击者访问运行在同一服务器上其他用户的隐私数据；抢占攻击者大量的占用资源导致其他用户无法正常获取服务[24]。

3) 数据存储安全

传感云中的数据存储在云端增加了数据保护的难度。对用户而言，数据存储在外部设备，增加了数据被篡改或泄露的风险。对传感云管理者而言，既要确保数据所有者的一般权限，又要保护数据不被恶意用户非法访问或窃取。除此之外，设置较高灵活度且明确的安全保障机制，提供更加透明的数据存储模块，实现合理数据利用和存储是必要的。

2.1.4 数据服务阶段

在数据服务阶段，主要存在访问安全和差异性安全。

1) 访问安全

虽然云计算和传感网的结合为用户提供数据共享和按需服务的平台，但是隐私数据的机密性受到挑战。在传感云应用过程中，不同等级用户，可访问的数据权限不同，且同一等级的用户访问数据的权限也有所差异。例如，医疗传感云应用中，医生可以访问部分病人的病理信息，而病人只能查看与自身相关的医疗数据，且不同医生可查看的病人信息的数量和对象也不完全一致。因此，在确保用户服务质量的基础上，如何制定基于角色的数据访问方案是传感云系统必须解决的安全问题。

2) 差异性安全

由于传感云服务内容的差异性和用户群体的差异性，服务安全的需求也不尽相同，单纯地设置统一的安全配置不仅会导致资源的浪费，也难以满足所有用户的需要。因此，需要根据服务模式、服务内容等设计个性化、多层次的安全保障机制。在设计过程中，综合考虑服务特性、复杂度、可扩展性等因素，设计具有较高灵活度的安全模块的传感云系统是未来发展的趋势。

2.2 基于虚拟化的安全问题

虚拟传感层安全是由传感云系统衍生出的新的安全问题。相较于传感网和云计算，传感云衍生出了虚拟传感层。本节根据虚拟传感层的特点，提出了几个传感云系统中新的安全问题。

虚拟传感层是处于传感网和云计算的中间层，为用户提供可视服务。虚拟传感层有 3 个特性：虚拟性、异构性和实时性。虚拟性是指虚拟传感层，是由非硬件设施构造出的中间层，如文献[21]中虚拟感知服务层。异构性则指虚拟传感层可以连接不同类型的传感网和云服务器，且可以为不同类型的终端用户（如手机、平板或电脑等）提供服务。实时性体现在为用户请求服务时，虚拟传感层是精准实时的获取用户所需数据，然后进行加工处理后提供给用户。因此，从这 3 个特性中，本文提炼出了 3 类安全问题：软设施安全问题[22]、对象可信问题[23]和数据共享安全问题。

1) 软设施安全问题

软设施安全问题主要包括系统安全和逻辑安全。系统安全主要体现在传感网服务商、云服务提供商等管理者和用户等第三方在使用传感云系统时，无法对系统造成安全威胁，或在攻击者恶意破坏系统时，如何保障虚拟层能正常运行。逻辑安全则指感知数据转化为服务的过程中，数据源与虚拟节点和服务对象的逻辑正确性不受外界干扰。例如，当恶意用户通过了身份认证，通过获取服务的渠道对系统发起攻击时，其他用户的服务不受其干扰。

2) 对象可信问题

传感云是一个具有综合性功能的系统，包含不同种类的传感网和云服务，因此，经常采用多个不同感知服务提供商和云服务提供商。如果不对服务商的可信问题进行估算和管理，当可信度较差的服务提供商被选用时，不仅会降低传感云的服务质量，如时延高、可用性差等，而且存在提供商利用其特权窃取用户的隐私信息的风险。另一方面，用户间的数据共享和传输依赖于用户的访问控制协议，为防止数据被篡改和泄露，用户间的可信关系需要定义和管理。此外，服务提供商对第三方软件的安全性难以实现完全认证，为防止恶意代码对系统的影响，建立相应的第三方软件可信性分析也是必不可少的。

3 传感云安全技术

通过对传感云安全问题的分析，本节给出保护传感云安全的 5 个关键技术：认证机制、加密机制、访问控制机制、预防和探测机制及可信计算与评估机制，分别从概念、原理和研究现状进行讨论。

3.1 认证机制

认证机制是对传感云系统中各个对象身份进

行验证，只有身份合法的对象才能正常工作，该机制保护系统受到伪节点、伪服务器、非法用户等安全威胁。

在传感层，物理节点都需要在网络中进行注册，并有唯一的标识对其进行身份认证。当有节点失效或新的节点加入网络时，都能够被虚拟传感层监控到。如果出现节点被捕获控制做出异常行为或伪节点加入网络、制造网络阻塞等非法行为，虚拟传感层能够及时定位和解决这类异常节点。在虚拟传感层，虚拟传感器节点的生命周期从用户请求生成的模板开始到用户撤销服务后结束。在工作期间，虚拟节点是用户和物理节点衔接的桥梁，安全认证机制是保障数据安全和服务安全的基础。在用户层，安全认证机制则主要指用户身份认证。不同用户访问的数据不同，根据用户身份，访问数据的权限也不同。有了多层次认证机制，可以在实现高服务质量的同时确保数据安全。

虽然目前认证手段种类繁多，如静态密码、短信密码、双因素认证等，但并不是所有的认证方法均适用于传感云系统。文献[25]认为传感云系统中的传感层比传统网络更易被攻击，提出一种改进的相互认证密钥协议，可防止离线密码猜测攻击。

3.2 加密机制

加密机制是以某种特殊的算法改变原有的信息数据，使未授权的用户即使获得了已加密的信息，也无法了解信息的内容。只有在输入相应的密钥之后才能显示出本来的内容，是数据安全中至关重要的方法[26,27]。

加密建立在对信息进行数据编码和解码的基础上。目前，加密分为对称加密和非对称加密，在对称加密中，双方采用共同的公钥和密钥，公钥用于加密数据，私钥用于解码加密后的数据；在非对称加密中，双方具有相同的公钥，但是私钥不同，只有私钥正确才能解码加密后的数据。

文献[28]基于云计算环境中数据流模型，提出了一种数据流安全框架，如图 4 所示。数据流动在传感云的 3 个层次中，且每层数据操作都不一样。在感知层，主要实现物理世界感知和数据收集，然后将收集到的大量数据进行聚合、压缩和过滤后传给网关。为了保证数据传输的一致性，网关对数据进行散列加密后，上传给云服务器。一些安全需求较强的应用会将数据分开存储，部分数据保存在本地并加密，其他上传到云服务器。存储在云服务器端的数据，将会被管理者使用和监控。当用户需要服务时，会将对应的数据提供给用户。文献[29]提出数据隐私保护和审计隐私性保护。数据隐私性保护指用户数据的隐私保护，如用户信息、数据的查看、操作等信息。审计隐私性保护则是一些重要的数据聚合结果，如静态数据计算、多项式方程输出等。

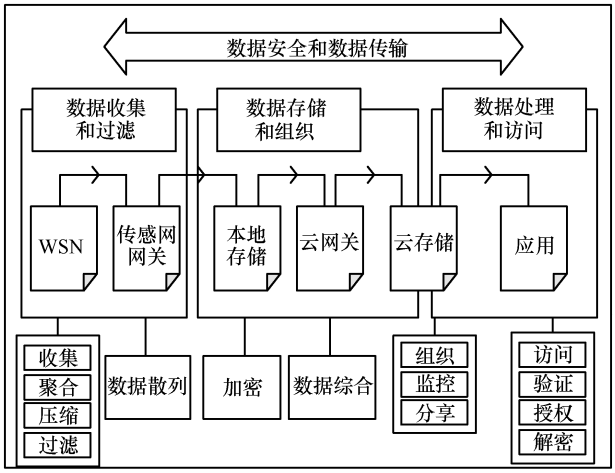


图 4 基于云环境的数据流安全框架

3.3 访问控制机制

访问控制机制是指主体访问客体的权限以及使用传感云系统和系统资源的过程。

访问控制机制主要实现 3 种功能：1) 防止非法对象访问受保护的网络资源；2) 允许合法用户访问受保护的网络资源；3) 防止合法用户对受保护的网络资源进行非授权访问。访问控制可分为 2 类：自主访问控制和强制访问控制。自主访问控制是指用户有权对自身创建的访问对象，如文件、数据等进行访问，并可将这些对象的访问权限授予其他用户。强制访问控制，则是由系统对用户所创建的对象进行统一的强制性管理，按照规定决定各类用户可获得的访问权限。

常见的实现策略有基于对象的访问控制模型（OBAC）、基于任务的访问控制模型（TBAC）和基于角色的访问控制模型（RBAC）。其中，RBAC 模型在传感云安全保护中最为常见，如文献[30]和文献[31]。

3.4 预防和探测机制

预防和探测机制是指传感云系统设计一系列规则和特征点对系统中对象合法性进行定义。

当前攻击手段主要有被动攻击和主动攻击 2 类，被动攻击主要是对用户或节点信息进行收集

而不是访问，如信道监听、非法复制文件等，从而造成感知数据和用户信息的泄露。这类攻击数据所有者无法感知到，因此很难探测，重点在于如何预防此类攻击。主动攻击则侧重于对数据进行篡改、伪造和中断系统。篡改通过修改感知层数据、替换虚拟传感层中软件服务中的程序、修改审计结果等操作破坏了传感云系统的完整性。伪造通过在感知层放置伪物理节点、传输信道中插入伪写数据、虚拟传感层写入伪代码等操作破坏传感云系统服务的真实性。中断系统的典型的攻击如拒绝服务攻击，会造成传感云系统无法正常工作。当系统被攻击时，传感云系统则需要对攻击进行探测和定位，并设置补救措施来保护数据和系统。因此，对于传感云安全而言，预防和探测机制是必不可少的。

在目前已有的传感云安全研究中，主要从预防的角度来保护传感云安全，且预防的机制还不够完善。本文认为，传感网和云计算个体的探测和防御研究可以作为研究传感云安全的参考。如文献[32,33]对传感器网络中入侵探测系统的研究，本文认为入侵监测系统是工具、方法和资源的结合，然后去鉴定、评估和报道入侵。一些防止入侵的方法（如加密）是保护系统的第一道防线。入侵检测系统是在第一道防线失败后保护系统的第二道防线，等同于小偷被发现后的警报作用，且入侵监测系统需具有常态变量计算为异常现象的低错误率和异常现象计算百分比的高正确率。文献[34,35]探索了云计算中最新发展入侵探测保护系统（IDPS）和警报管理技术，并提供了一种易于理解的入侵分类和可审查的解决方法。

3.5　可信计算与评估机制

可信计算与评估是指通过一定的方式计算对象的可信度，进而评估该对象工作的模式和范围。

在传感云系统底层，不同类型的传感网来自不同的传感网提供商，提供商的可信度均有所差异，如何对提供商的信誉进行评估是确保传感云安全的基础。传感云中的云服务器提供商的评估和选择也面临同样的问题。另一方面，在传感云工作期间，对于微小模块的可信计算和评估同样不可或缺。例如，传感云底层物理节点是否可信，影响了数据的完整性、可用性和有效性等方面。当前关于可信计算和评估的研究存在一个关键问题，那就是可信评估标准不一致，导致评价体系可用性差。在复杂的传感云系统中，设计一套实用有效的可信计算与评估方案来抵御恶意攻击很有必要。

4　已有的解决方案

目前，已有的安全解决方案可以从产业传感云和研究传感云这 2 个方面分析。产业传感云，如目前已有的传感云系统，Xively[36]、SensorCloud[37]、SensaTrack[38]、NimBits[39]和 ThingSpeak[40]等。研究传感云则是有关传感云安全解决思路的研究文献。

4.1　已有的传感云系统

Xively 平台（原名 Cosm 和 Pachube）是纳斯达克公司的一部分，为全球性公司提供远程访问和合作产品，提供链接产品管理的解决方案。通过 Xively 云平台，可将设备、数据、用户连接在一起，从而实现与物理世界的交互。Xively 平台有 5 个关键特点：1) 为所有类型的设备（如工业、环境等）提供灵活、安全的连接方案，无论是小型传感器（烟雾探测器等）还是大型集装箱；2) 提供大量的工具完成综合的数据管理，提高服务质量；3) 提供预配置权限和包括平台在内的组织层次结构，对用户、设备、数据可见性等进行安全管理；4) 提供特定的安全专家来防范设备克隆、DDoS 攻击和未授权的访问或控制；5) 确保用户产品及数据的安全存储，完善连接设备自身存在的安全漏洞。

SensorCloud 平台是一个独特的传感器数据存储、可视化和远程管理平台。利用强大的云计算技术提供良好的数据可伸缩性、快速可视化和用户编程分析功能。该平台主要有 4 个特点：1) 安全性，所有数据和事务发生在传输层安全性（TLS），该平台建立在 Amazon Web 服务，提供了一个世界级安全和信任的平台；2) 为任何设备和应用提供了稳定的开源数据 API；3) 提供警报功能，允许用户为监测数据溢出和感兴趣事件创建自定义邮件和短信提醒；4) 实时连接，允许自身设备与 WSDA 网关和对应的传感器相连。

Nimbits 平台是一个开源且免费物联网平台。在该云平台上，可以搭建自己的服务器并扩大到任何尺寸。Nimbits 服务器是一个 Web 服务器，提供了读写数据、创建对象、触发器和订阅的 API，旨在帮助用户设备可互相连接和交互。该平台主要有 3 个特性：1) 触发器，当新的数据被记录时，可以

触发一个基于数据点的事件，该事件可触发 Web 钩、计算、E-mail 和其他基于事件描述的事件；2) 数据点，Nimbits 中的数据点类似于数据的桶或主题，包含了由数字、文本或 GPS 坐标组成系列时间戳值，所有数据以树结构存储在 Nimbits 中来简化检索；3) Java/Android Client，为用户提供搭建客户端、服务器或安卓 APP 的库。

ThingSpeak 平台是一个物联网平台，可以收集传感器数据并存储在云端并发展成物联网应用程序。该平台有 5 个特性：1) 灵活数据传输信道，既可以为用户创建隐私信道收集数据，用户也可以通过公用信道读取数据；2) REST 和 MQTT API，REST API 可以申请创建或更新 ThingSpeak 信道和图表，MQTT API 可以更新信道；3) Matlab 分析和可视化，使用 Matlab 分析软件分析数据，且可以把数据写入通道或创建可视化；4) 提供使用应用来转换、虚拟化数据或触发动作；5) 事件调度，提供基于时间控制的事件调度策略。

Arrayent 平台为消费者提供传感云 PaaS 服务，主要有以下 3 个特性：1) 链接云服务，以最少的开发快速链接产品；2) 洞察服务，从用户和产品使用数据中获取关键信息；3) EcoAdaptor 服务，通过产品和服务间的云集成和互操作性提高产品的价值。该平台主要有 3 个优势：1) 链接云是专为消费产品制造商搭建的架构，具有高度安全性和伸缩性；2) 根据对数据的分析来理解消费者行为，为用户提供安全的数据访问和兼容主流的数据分析环境；3) 以安全和可扩展的方式加快第三方认证过程且降低了制造商对数据的占用时间。

Digi 平台是一种机器对机器（M2M）的通信平台，主要提供的服务有以下 3 点：1) 远程管理服务，简化设备部署和管理设备以满足性能义务和安全性要求；2) 设备云服务，从边缘设备和平台访问和整合数据；3) 无线设计服务，提供无线连接技术和资源。该平台使用户搭建无线产品尽可能简单和安全，且采用严格安全兼容的规定保护野外的产品和网络。

YeeLink 平台提供高并发接入服务器和云存储方案，能够同时完成海量的传感器数据接入和存储任务，确保数据能够安全保存在互联网上；提供先进的鉴权系统和安全机制，能够确保数据只在用户允许的范围内共享。

表 1 对这些平台采用的安全机制进行对比分析，共给出了 7 类安全指标：通信安全、物理安全、访问安全、存储安全、可信安全、服务安全、共享安全。根据传感云的 3 层体系结构，这些安全指标可以分为 3 个部分。物理层的安全指标有物理安全和通信安全，物理安全是保障物理节点不受破坏和伪节点替换，通信安全则是保护数据在传播和上传过程中不受监听和篡改。虚拟传感层的安全指标有可信安全和共享安全，可信安全是指确保所有的传感器节点、虚拟节点、云服务是合法的，共享安全则是确保用户间的数据是合法且独立的。云服务层则包含访问安全、存储安全和服务安全，访问安全则是确保用户在不同身份时，访问数据权限合法，存储安全是感知数据安全和用户数据安全，服务安全则指服务的可靠性。从表 1 可知，物理安全、通信安全和共享安全是传感云平台的关注重点，而访问安全和服务安全的实现度则较低，这 2 类安全指标均在云服务层。由于传感云系统应用领域的不同，不同的传感云系统的安全需求有所差异，因此，实现统一的云服务层安全难度较大。

4.2 传感云安全相关研究

根据研究解决的不同安全问题，本文将目前对传感云安全的研究分为 5 个方向：基于数据的传感云安全研究、基于服务的传感云安全研究、基于信任的传感云安全研究、基于虚拟化传感云安全研究

表 1 **产业传感云安全对比**

传感云平台	通信安全	物理安全	访问安全	存储安全	可信安全	服务安全	共享安全
Xively	√	√	—	√	—	√	√
SensorCloud	√	√	—	—	√	—	√
NimBits	—	√	—	√	—	—	√
ThingSpeak	√	—	—	√	—	—	√
Arrayent	√	√	√	—	—	—	√
Digi	√	√	—	—	√	—	—
YeeLink	√	√	√	√	—	—	√

和基于恶意使用系统的安全研究。基于数据的传感云安全研究主要解决传感云中数据安全存储、数据安全访问和数据安全传输问题。基于信任的传感云安全研究主要解决传感云中物理节点妥协攻击、伪基站、伪服务器攻击的安全问题。基于虚拟化的传感云安全研究主要解决虚拟化带来安全问题研究，如虚拟层软设计攻击、用户恶意操作攻击。下面，将根据相关文献做详细介绍。

4.2.1　基于数据的传感云安全

文献[41]在基于医疗传感云的数据管理中，提出了一个创新的框架来实现有效的、弹性的安全机制，确保数据的机密性、完整性和良好的访问控制。作者认为基于属性的加密机制（ABE）有 2 个弊端。虽然 ABE 不需要存储服务器就可以对数据加密，但是在 ABE 加密策略中，密文可以被任何持有密码的人解密并访问数据，这样导致当访问策略改变时，本身无权访问数据的人却可以访问数据。另一方面，ABE 是由密钥和访问结构管理组成，问题是访问结构由谁设计，密钥由谁产生和分配。通过 ABE 在医疗传感云存在的问题，作者提出使用对称密码学和 ABE 共同加密数据。首先，随机产生一个对称密钥（RSK）对文件进行加密，接着，使用 ABE 对 RSK 进行加密，然后，加密的文件和加密的 RSK 上传到云服务器存储，为认证的用户提供数据分享。图 5 是文献[41]中给出的医疗传感云安全案例。

文献[42]研究了传感云在智能网关应用中的大数据信息管理问题，并提出了建设异构云计算中心来提供不同种类的云服务，信息管理和大数据分析。在智能网关的安全方面，采用基于身份的加密和基于身份的签名方案来保护数据安全。图 6 为基于身份的加密方法的框架。

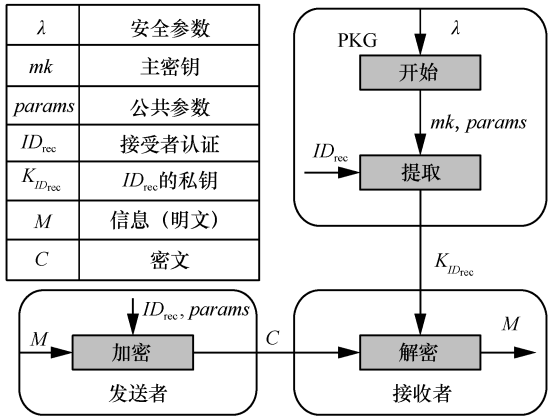


图 6　基于身份的加密方法的框架

在基于身份的加密方案中，可信的第三方拥有私钥生存器（PKG），首先，生成主密钥 *mk* 和公共参数 *params*，*params* 需要告知每个相关的团体。PKG 采用提取算法根据身份信息 ID_{rec}、密钥 *mk* 和公共信息 *params*，提取出身份为 ID_{rec} 对应的私钥。发送方将信息、接受者 ID_{rec} 和公共信息 *params* 发送给接收方。当接收方收到私钥时，才能对密文进行解密。密钥生成器 PKG 根据安全参数生成主密钥和公钥参数，然后采用提取算法计算身份 ID_{rec} 对应的私钥。签名者用私钥和公共参数对信息进行签名。检验者根据身份 ID_{rec} 和公共参数 *params* 对签名进行检验是否有效。

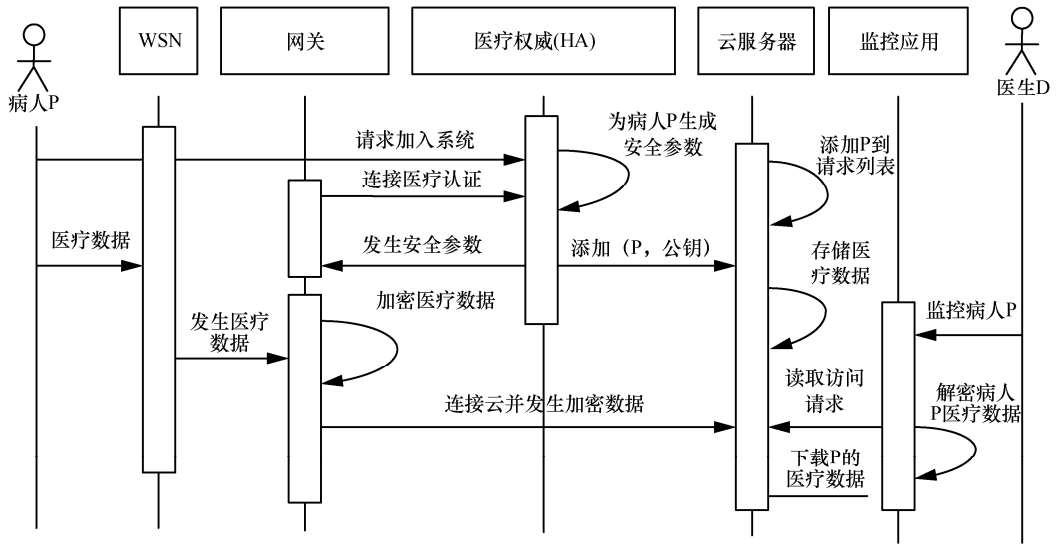


图 5　医疗传感云安全案例

4.2.2 基于服务的传感云安全

文献[43]采用基于传感云多层认证机制为多用户提供安全的服务，认为不同终端设备的认证是其访问公共网络的基本要求。大部分已经出现的认证方案不适用于传感云，因为节点和用户规模较大，且传统的认证方法对时延要求较高的应用服务的影响较大。另一方面，由于云计算为用户提供计算和存储功能，因此，认证的解决方案有必要涵盖整个系统。作者提出了多层认证机制则是在文献[44]的基础上的一个加强版本，响应者和终端用户均通过云服务器进行认证，其中用到了公钥密码学算法——椭圆曲线数字签名算法和椭圆曲线赫尔曼密钥交换算法，整个安全机制有 3 个阶段。在初始化阶段，主要实现密钥生成和分配。在注册阶段，用户发送请求信息给云服务器进行注册，请求信息包含注册信息和用户 ID 对应的公钥加密信息。在认证阶段，首先，用户发送含有 ID 索引的散列值、证书 CertU 和时间戳 TU 给云服务器。如果云服务器验证成功，则将云服务器身份、时间戳和 MAC 地址发送给传感网网关。如果网关认证成功，则将网关本身身份、时间戳和 MAC 地址发送给确切的传感器节点。如果传感器节点认证成功，则按原路返回用户需要的信息，如图 7 所示。

文献[45]主要通过认证和访问控制来实现安全可靠的传感云服务，采用基于身份的加密认证来简化密钥分配和认证过程。基于身份的加密使用独特的公钥识别认证和签名验证，大大降低了密钥管理的复杂性。同时，有 3 点需要注意：1) 用户的身份是唯一的；2) 当一个身份产生时，对应分配一个虚拟传感器节点和虚拟传感器节点组；3) 用户层和虚拟传感层各有一个密钥生成器（PKG）。该安全方法主要由 2 个部分组成，密钥的生成及基于身份的加密和数字签名。

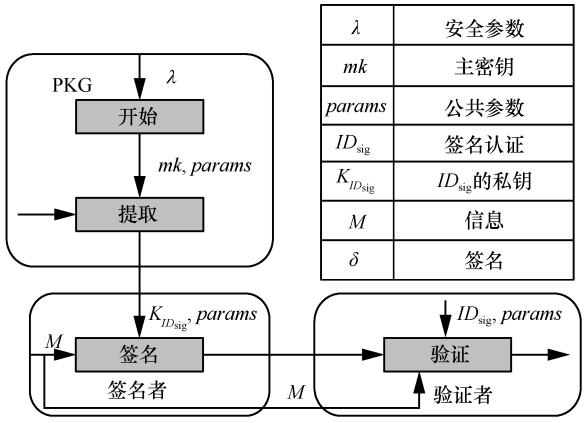


图 7 基于身份的签名方案

4.2.3 基于信任的传感云安全

目前，关于传感云可信计算和评估的研究主要有传感网和云服务提供商的可信评估和计算；传感网底层节点的可信评估与计算[46]。

文献[47]提出了一种有效的分布式可信模型（EDTM）来抵制传感云底层网络的普遍攻击，其基本结构如图 8 所示。EDTM 包括 2 个主要的组件，单信任模型和多信任模型，包括以下 6 个部分：直接信任模块、推荐信任模块、间接信任模块、集成信任模块、传播信任模块和更新信任模块。当一个主观节点想获取一个目标节点的信任值时，它首先检查记录邻居节点的列表。如果对象节点的 ID 在邻居节点列表中，触发单信任模型。在单信任模型中，如果信任计算完全基于目标节点和主观节点的经验，这个模型被称为直接信任模型。否则，推荐信任模块建立。在多信任模型中，当主观节点接收到其他节点的推荐信任时，间接信任模型建立。在

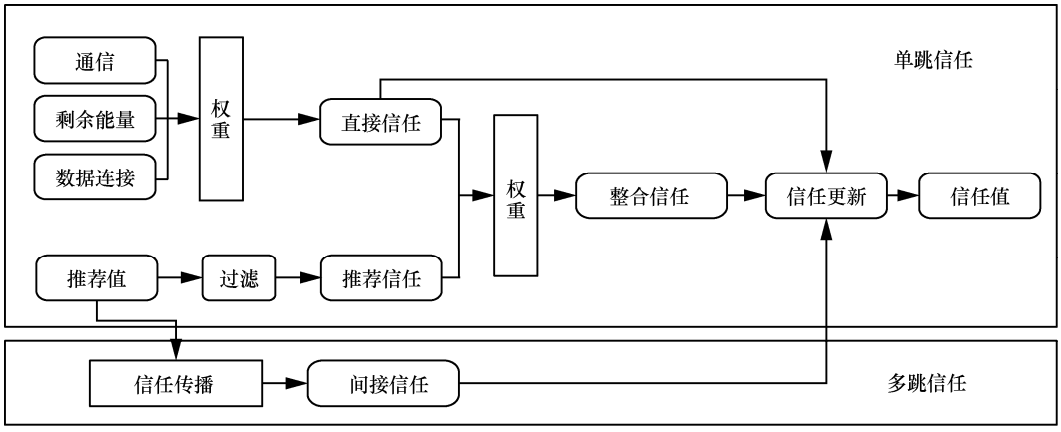


图 8 分布式信任框架

当前信任模型中，直接信任和推荐信任总是用来评估传感器节点的可信度。直接信任的计算是基于 2 个邻居节点之间的通信行为。然而，由于恶意攻击，只使用直接的信任评估传感器节点并不准确。因此，其他传感器节点的推荐改善信任评估的准确度。此外，如果 2 个邻居节点之间的通信数据分组的数量太小，它很难决定目标节点的好坏。因此，在单信任模型中，作者定义一个通信数据分组阈值。如果目标节点和主观节点之间的通信数据分组高于阈值，计算直接信任即可。否则，需要推荐信任来对目标节点进行信任评估。

在多信任模型中，节点首先需要选择一组推荐节点。然后，基于推荐信任模型和传播信任计算模型来计算间接信任。

文献[59]中，作者认为对云服务商（CPS）和传感网提供商（SNP）基于认证的可信信誉的计算和管理存在 2 个重要的漏洞。一方面，恶意攻击者可以扮演真实的云服务提供商与传感云系统进行通信，或假冒传感网提供商与云服务商进行通信，造成系统无法从假冒的提供商获取任何有用信息，同时，真实的提供商的可信度和信誉值被影响了。另一方面，没有可信和信誉计算、管理，低信誉的服务提供商无法被识别，造成系统漏洞。为了解决这 2 个问题，作者分析了 CPS 和 SNP 的认证问题，并提出了一种适用于传感云的创新可信认证和信誉计算管理方案。该方案可实现对云服务提供商和传感网服务提供商的可信认证，帮助传感云系统选择真实可信的 CSP 和 SNP。

文献[60]提出了一种基于簇的可信扩散和能量有效的计算方案。本文认为能量是传感云系统不可忽视的部分，单一考虑安全而忽视能量的可信方案无法被应用到实际中，因此，他们将可信管理和最大化能量效率融为一体。不仅如此，该方法还考虑了移动元素可能给传感云系统带来的安全威胁，并设计对应的安全机制来保护系统。

4.2.4　基于虚拟化传感云安全研究

传感云安全系统中，虚拟化对安全带来新的挑战，在文献[61,62]中，采用虚拟化工具跟踪数据的传播路径和实现点对点的通信，从软设施的角度，对传感云的系统安全建设提供了一种新思路。文献[63]利用云计算的软件定义层，提出了一种事件响应的虚拟云计算结构，如图 9 所示。相较于传统的云计算，该结构既支持在软件定义层实现数据处理，也支持在近端网络实现数据处理，这种机制增强了实时类应用的可靠性和安全性。这种思路借鉴了雾计算的思想来协助云层管理传感云系统虚拟层，降低了传感云系统对云层的依赖性，为传感云系统防御来自云端的攻击提供了新思路。

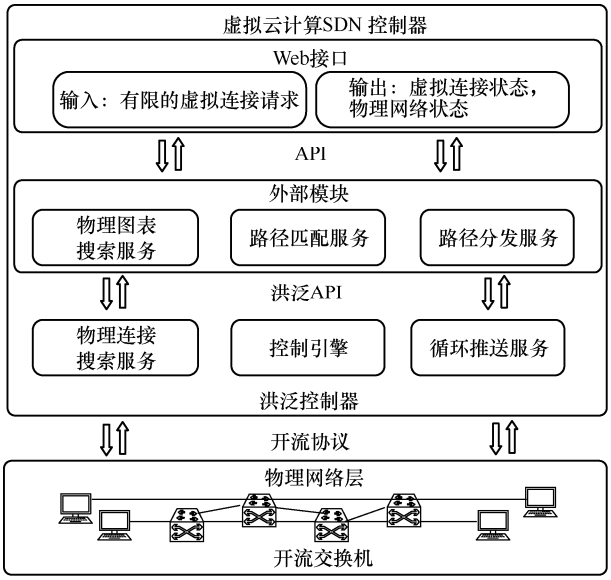


图 9　虚拟云计算系统原型

4.2.5　基于恶意使用系统的安全研究

加强安全认证机制和提高系统健壮性是目前解决恶意使用系统问题的主要研究方向。

文献[64]提出了结合可信技术的SDN架构的方案。该方案在没有任何可信第三方信任域间，设计了一种自治系统的身份认证协议。通过禁止谓词逻辑和网络交互协议 AVISPA 安全分析工具，保证了协议的安全性，还可以提供完整的安全测试。文献[65]提出了一种附加加密信道和认证算法来保护无人机安全，该加密方法为保护合法用信息提供新思路。另一方面，文献[66]提出一种 BFT 容错云，BFT 容错云是在云计算环境下构建的一种强大系统容错框架。当资源提供者出现故障时，包括任意的行为失误，系统都能正常运行。文献[67]在驾驶辅助系统绝对安全的背景下，提出能容忍任何子系统出现故障的启发式任务分配和其搭建的软件容错框架，可以较好地实现系统的容错功能，提高了传感云系统在车载网领域的实现安全性。

4.3　分析比较

由于目前传感云安全研究的目的不尽相同，如基于穿戴设备传感云安全、基于智能医疗的传感云安全、基于军事服务的传感云等，安全需求多种多

样。本文对各类安全方法进行了分析比较对比。其中，表 2 为基于数据的传感云安全方法比较，表 3 为基于服务的传感云安全方法比较。

表 2 基于数据的传感云安全方法比较

方法	完整性	真实性	机密性	隐私性	审计安全	访问控制安全	存储安全
文献[47]方法	是	是	是	否	否	是	否
文献[48]方法	否	否	是	是	是	否	是
文献[49]方法	是	是	是	否	是	是	否
文献[50]方法	是	否	是	是	否	否	是
文献[51]方法	否	否	是	是	否	是	是
文献[52]方法	是	否	是	否	是	否	是
文献[53]方法	否	否	是	否	否	否	是
文献[54]方法	否	否	是	是	否	是	是
文献[55]方法	否	否	是	是	是	否	是

表 3 基于服务的传感云安全方法比较

方法	认证机制	加密机制	签名机制	审计机制	权限管理机制
文献[49]方法	是	是	否	否	是
文献[50]方法	是	否	否	是	是
文献[51]方法	是	是	是	否	是
文献[56]方法	是	是	否	是	否
文献[57]方法	是	是	否	否	否
文献[58]方法	是	否	否	否	是

综合表 2 中的对比可以看出，目前，基于数据的传感云安全方法存在以下 2 个问题。1) 大部分方法虽然考虑了数据的机密性，并在数据完整性、隐私性、审计安全、访问控制和存储研究方面有部分涉猎，却都不够完善。这说明目前对传感云安全的研究还处于起步阶段，还有很多安全威胁及系统漏洞有待研究和解决。2) 很少有研究对数据的真实性进行考量。该问题可以通过底层物理节点的身份认证和虚拟传感层对物理节点的监控来确定数据来源和数据真实性，如果在监测期间内，节点身份确定，且无异常行为，则可以确定当前节点上传数据的真实性。反之，则需要进一步验证。

综合表 3 中的对比可以看出，大部分基于服务传感云安全均采用认证机制来确认身份是否合法，并通过权限管理来控制用户能够访问数据的广度和深度，部分采用加密机制对数据进行加密，并对计算结果进行验证后才提供给用户。小部分方法采用签名机制，可能由于签名方法主要功能在实现文件共享时，所有者可以采用签名的机制确保自身。

而在传感云系统中，用户只拥有自身的隐私数据，且该数据无法与其他用户共享，同时底层的感知数据不归用户所有，因此，基于签名机制的方法对传感云安全不是很适用。

表 4 对比了可信计算和评估的传感云安全方法，主要从研究的信任对象和攻击类型这 2 个方面比较。CSP、SNP 分别指云服务提供商和传感网服务提供商。DOS、BMA、OOA、SA、COA、CA 分别指否认服务攻击、差评攻击、on-off 攻击、女巫攻击、合谋攻击和伪造攻击。从表 4 可以看出，目前对传感云底层网络中节点的可信度研究较多，小部分研究云服务商和传感网服务商的信誉度。在防御的攻击类型方面，研究方向较为分散，没有一种全面的方法。因此，未来传感云安全在可信计算和评估方向还需要继续深化、规范、统一。

基于以上文献对传感云安全的研究，从广度来讲，有 2 个研究方向：基于数据的传感云安全研究和基于服务的传感云安全研究，本文在后面章节对传感云安全未来的研究做了更详细的分析和讨论。从深度来探讨，目前已有的传感云安全方法，大部分是提出了一个安全框架，讲解了框架能够实现的功能，但是很少研究详细说明框架中每一层如何实现，并提出一种扩展性和兼容性良好的解决方案。因此，根据以上 2 点分析及第 1 节对传感云安全的

表 4 基于可信计算和评估的传感云安全方法对比

方法	信任对象			攻击类型					
	CSP	SNP	传感器节点	DOS	BMA	OOA	SA	COA	CA
文献[53]方法	—	—	√	—	√	√	—	—	—
文献[65]方法	√	√	—	—	—	—	—	—	√
文献[66]方法	—	—	√	—	√	√	—	—	—
文献[68]方法	—	—	√	—	—	—	—	√	√
文献[69]方法	√	—	√	√	—	—	—	—	√
文献[70]方法	√	—	—	√	—	—	—	√	—

调查可知，目前传感云安全处于一个起步阶段，只有设计出一个完善并详细的传感云安全系统，才能实现快速发展并应用到更多的领域。

5　未来的研究方向

根据传感云的安全需求，目前已有的解决方法还不够完善，均是针对传感云中部分安全问题提出的解决方案，如基于数据隐私保护安全框架、基于访问控制安全机制等。对于传感云系统整体安全问题，还有许多亟待解决的安全问题。本文将尚未被广泛讨论和研究的安全问题或解决方案作为未来的研究方向，具体有以下 5 点。

5.1　基于虚拟化建设的传感云安全

基于虚拟化建设的传感云安全是从管理的角度保护传感云系统。一方面，虽然传感云系统是传感网和云计算的结合的产物，但其本身与后两者相比具有一定的差异性，例如，传感云系统衍生的虚拟传感层中虚拟节点与物理节点的逻辑关系，因此，传统的桥接传感网和云计算的建设模式并不完全适用于传感云系统，有必要设计一套适应传感云系统特性和安全需求的软件设施，如虚拟层管理系统、开发工具等，为保护传感云系统安全提供有效的解决方法。这也是未来值得研究的新方向。

5.2　基于可信计算和评估传感云安全

分布式协作和信息共享是传感云系统必要的操作，为了实现对物理环境的有效监测并将数据加工为有效服务，所有参与者应该是可信的。然而传感云底层网络常工作在无人看管的环境，导致系统安全受到威胁，易受到节点捕获攻击、干扰攻击、伪节点攻击等，对数据的完整性、机密性和可用性有着极大的影响。当前关于可信的研究还不够全面，无法采用到实际应用中，因此，传感云安全的可信计算和评估依旧是未来研究的热点问题。第 6 节将给出基于雾计算框架的可信计算与评估的解决方法。

5.3　基于低耦合的传感云安全

目前，已有关于传感云安全的研究主要集中于数据的安全隐私性保护和传感云服务安全，并没有考虑到传感云为多用户提供服务时，当多用户同时进行操作时，会产生不安全因素。这种不安全因素如下。首先，多用户使用不同的虚拟传感节点，公用部分相同的物理传感器节点，造成当传感器节点同时接收到不同命令时，出现冲突；其次，多用户获取服务时共用同一个虚拟传感节点，从而共用所有的物理传感器节点，导致用户对服务的反馈命令出现完成耦合。因此，设计一个低耦合的传感云安全框架，要尽量避免耦合的状况发生，并在耦合发生时，尽量减少耦合带来的不安全因素。

5.4　基于容错性的传感云安全

传感云中的故障和错误主要有 3 个源头：底层物理监测错误，虚拟传感层聚合或计算错误及用户服务错误，这三者既可以是递进的关系也可以独立存在。对于底层物理监测错误，可能由于物理节点故障或能量耗尽而失效或节点被攻击者捕获后，恶意提供错误信息，该问题可通过虚拟传感层对物理节点的监控和管理来判断物理节点的状态和异常行为，进而设计补救机制。对于虚拟传感层聚合或计算错误，可能由于攻击者对云服务器进行入侵，改变云服务器的计算和存储模式，进而伪造虚假计算结果提供给用户，该问题需要对所有的云服务器提供商进行认证，且对云服务器的计算结果进行安全审计以实现防御和容错的目的。对于用户服务错误，可能由于用户请求出现耦合，导致服务资源提供出现冲突，该问题可以通过设计低耦合安全机制来减少用户需求耦合的可能性，并在出现耦合时，提供改善的方案。

5.5　基于数据存储和恢复传感云安全

在云端环境中，被上传的数据不在其所有者的直接掌控之下，因此，必须加以检测来保证只有授权用户才能访问这些敏感数据，而包括云服务提供商在内的其他人不应该在未授权情况下获得任何有关数据信息。数据所有者必须掌握全部的存储数据的访问权和云服务，理论上杜绝了任何数据泄露给其他人的可能性。上传至云端的数据必须被正确和可信地存储，这也就意味着它不能被非法或不正当修改，故意删除或伪造。通常它还结合一些审计手段，以便所有者可以在任何不正当操作发生时及时检测到。数据可用性代表合法用户只要愿意就可以访问所需数据。同时保证数据在任何情况下都可以按用户要求的标准提供并可用，这意味着在发生灾难性事件时，有相对应的措施用来进行数据恢复。

6　基于雾计算框架的传感云安全

雾计算（fog computing）模式是云计算模式的延伸，在 2011 年由思科（Cisco）首次提出[71]。相比云计算模式而言，雾计算的特点是雾层更贴近末

端节点、具有一定的本地计算存储能力、更广的地理分布和移动性支持[72]，因此，能更好地直接管理和控制传感器网络中节点，并作为联系底层和云层服务的桥梁和纽带，该新型计算模式正好可以弥补云计算模式中部分安全漏洞。

本文提出了一个基于雾计算的传感云系统框架，如图 10 所示。最上层为云计算层，提供强大的计算服务和存储服务。第二层是由少量移动节点组成的雾节点层，雾节点层作为联系传感器网络与云端网络的纽带，主要进行移动节点之间的协作与配合、桥接传感器网络与云、管理机密性数据的存储。一些本地化的、实时性要求高的计算任务将放在雾节点层处理，同时雾节点也能存储少量数据[73]。雾节点之间构成一个虚拟的网络，相互之间的通信可以是直接的，也可以是借助普通传感器节点间接信息传递。底层为传感网络层，提供感知数据。且该模式基于传统的、固定节点组成的传感网，引入的少量移动式节点不会造成太大的成本开销。

安全方法新思路如下。

相比于第 2 节提到的传感云系统，基于雾计算框架的传感云系统中，有了本地移动节点，更好地管理、分配、调控底层的物理节点，同时，为传感云安全提供了新的解决思路，本文主要从以下几点讨论。

6.1 入侵探测与防御安全

本文认为可以利用雾计算框架来优化传感云系统的入侵探测和防御机制。在典型的基于雾计算框架的传感云系统中，雾层节点本身就具备一定的计算、存储、移动能力，而且接近传感器网络层，能够更好地直接管理和控制传感器网络中的传感器节点。因此，入侵探测和防御机制所需要的计算和存储资源完全可以由雾层节点来提供从而避免了数据要直接和云端交互产生的高时延问题。当计算需要更多的资源时，雾层节点也可以将大部分需要计算的数据上传到云端进行计算同时对病毒入侵进行先期的基本控制处理。这样做的好处是系统不必因为等待计算结果而延误补救时机。同时，由于雾层节点并非是将全部的计算数据上传云端，因此，增加了数据的私密性保护，降低了数据被攻击者破解和篡改的可能性。

6.2 耦合安全

本文参阅了大量文献，发现物理节点的耦合和操作系统中资源耦合有异曲同工之处。不同种类的传感器节点可以比作不同类型的资源，统计其数量，按一定规则分配可提高物理节点的利用率。虚拟节点类似于进程，一个虚拟节点的构建需要若干物理节点资源，且虚拟节点间的关系可分为 3 种：独立、包含和互斥，如图 11 所示。不同填充形状的传感器节点代表不同类型的传感器节点，构成 3 个虚拟节点 A、B、C。节点 A 和 B 间的关系为互斥，因为它们存在公共节点，但是也存在不同节点。A 和 C 之间为包含关系，因为构建成 A 的节点可以构建 C 节点。B 和 C 为独立关系，两者互不影响。

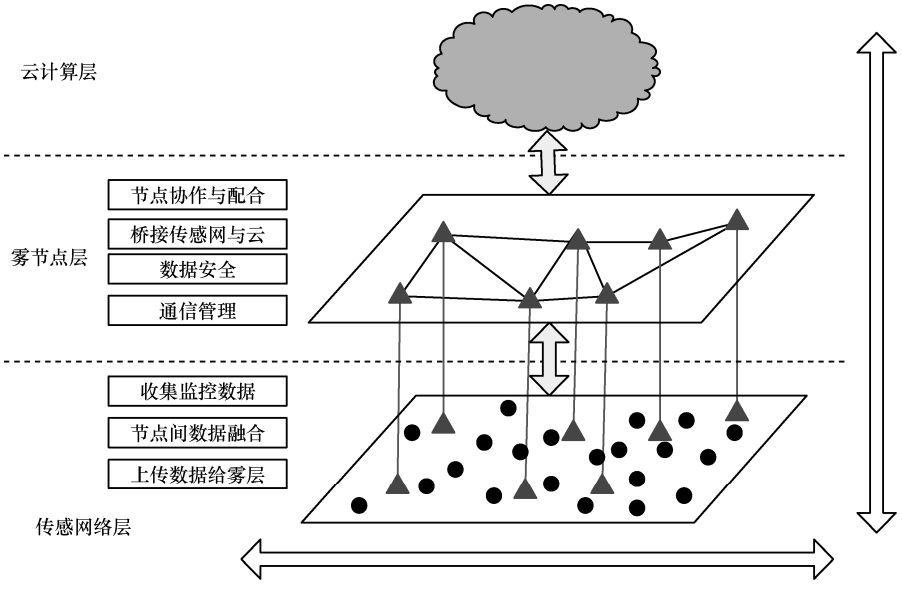


图 10 基于雾计算框架的传感云

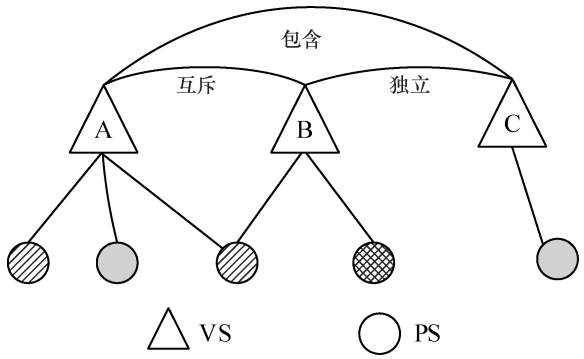


图 11　虚拟传感器节点间的关系

通过应用该模板，物理节点间的资源和命令耦合则可采用进程调度算法进行处理，主要遵循 3 个原则：1) 避免造成系统死锁；2) 服务命令执行顺序按照优先级算法设计执行；3) 保护用户隐私性数据。以上原则为本文对解决耦合安全的算法的设想，由于传感网的计算和能量有限，该设想需要雾层执行此算法，对虚拟传感层发出命令进行解析、应用算法模板、将解析后的命令发给传感层执行。

6.3　可信计算与评估

对目前有关传感云可信计算和评估的方法进行了总结，主要有 3 个问题：1) 研究的对象不够全面，还没出现对 CSP、SNP 和传感器节点同时评估的方法；2) 抵御对象不够全面，从表 4 可看出，普遍攻击的种类多、方式多样化，而目前的研究均只针对部分攻击；3) 信任的参考值不一致，不同的方法，有不同的信任考量标准，扩展性差，移植性差。另一方面，由于传感云底层网络有限的能量和通信能力，目前已有的传感云系统的可信计算和评估在方法设计上有诸多限制，如底层传感器节点的认证方法不可太复杂，可信评估计算不能太频繁，当云服务器参与可信评估时，通信量不能太大等，这些限制降低了可信计算和评估的准确度。

本文认为雾计算的加入可辅助传感云系统设计一套完善的可信计算和评估模型。雾层介于传感层和云层之间，可充当于中间管理层，提供各项参数收集，辅助计算等服务，为传感层和云层交互提供良性接口。

6.4　数据云存储安全

本文提出一个基于雾计算思想的安全云存储三级结构，来解决云存储中的私密性问题。其基本思想为利用纠删码技术将文件分块之后，将小部分存储在绝对安全的本机，再存储多一些的数据在相对安全的雾服务器中，最后大部分数据存储于云端。存储于本机的数据可以用来和雾服务器中数据结合还原部分关键数据，这部分关键数据又可以用来和云服务器中的数据结合来还原原始数据。值得注意的是，无论是云服务器中还是雾服务器中存储的数据，如果被恶意外来者获取了，都无法还原出原始数据。这种技术可以解决传统加密技术无法解决的很多问题，尤其是对于传感云服务内部攻击。

7　结束语

传感云系统是一个新的研究热点。传统的传感网在云计算的协助下通过实时感知物理世界并将数据上传到云端，为身处各地的用户提供便利的服务。然而，由于数据被上传到云平台，感知数据和用户信息被暴露给第三方，造成数据的隐私性泄露，机密性和完整性无法得到保障等安全问题。这些安全威胁严重阻碍传感云发展。虽然目前有部分国内外学者对传感云的安全问题进行了研究并提出了对应的解决方案，但是均不够全面和完善。本文首先给出了 3 种传感云实现框架，并结合几个典型的传感云应用，强调了传感云安全的重要性。然后对传感云面临的传统安全威胁和衍生的潜在安全威胁进行了探讨和总结。基于安全威胁的总结，本文提出了传感云发展中需要具备的安全需求。接着，对目前已有的传感云安全研究进行归类，对于每类方法，结合典型文献的实现细节，对现有方法进行分析、对比和总结，探讨了未来传感云需要研究的方向。最后，提出了基于雾计算框架下的传感云安全研究。

参考文献：

[1] 林闯, 苏文博, 孟坤, 等. 云计算安全: 架构, 机制与模型评价[J]. 计算机学报, 2013, 36(9): 1765-1784.
LIN C, SU W B, MENG K, et al. Cloud computing security: infrastructure, mechanism and model evaluation[J]. Chinese Journal of Computers, 2013, 36(9):1765-1784.

[2] 王国军, 王田, 贾维嘉. 无线传感器网络中一种基于行进启发的地理位置路由[J]. 传感技术学报, 2007, 20(2): 382-386.
WANG G J, WANG T, JIA W J. A travel-based position route in wireless sensor networks[J]. Journal of Sensor Technology, 2007, 20(2): 382-286.

[3] WANG T, PENG Z, LIANG J B, et al. Following targets for mobile tracking in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2016, 12(4):1-24.

[4] 张希伟, 戴海鹏, 徐力杰, 等. 无线传感器网络中移动协助的数据

收集策略[J]. 软件学报, 2013, 24(2): 198-214.
ZHANG X W, DAI H P, XU L J, et al. Mobility assisted data collection strategy in wireless sensor network[J]. Journal of Software, 2013, 24(2): 198-214.

[5] 俞姝颖, 吴小兵, 陈贵海, 等. 无线传感器网络在桥梁健康监测中的应用[J]. 软件学报, 2015, 26(6): 1486-1498.
YU S Y, WU X B, CHEN G H, et al. Application of wireless sensor networks in bridge health monitoring[J]. Journal of Software, 2015, 26(6): 1486-1498.

[6] DASH S K, SAHOO J P, MOHAPATRA S, et al. Sensor-cloud: assimilation of wireless sensor network and the cloud[C]//International Conference on Computer Science and Information Technology. 2012: 455-464.

[7] 刘正伟, 文中领, 张海涛. 云计算和云数据管理技术[J]. 计算机研究与发展, 2012, 49(1): 26-31.
LIU Z W, WEN Z L, ZHANG H T. Cloud computing and cloud data management technology[J]. Computer Research and Development, 2012, 49(1): 26-31.

[8] WANG T, LI Y, WANG G J, CAO J N, et al. Sustainable and efficient data collection from WSNs to cloud[J]. IEEE Transactions on Sustainable Computing, 2017, PP(99):1-12.

[9] 曾建电, 王田, 贾维嘉, 等. 传感云研究综述[J]. 计算机研究与发展, 2017, 54(5):925-939.
ZENG J D, WANG T, JIA W J, et al. Survey of sensor cloud[J].Computer Research and Development, 2017, 54(5):925-939.

[10] MISRA S, BERA S, MONDAL A, et al. Optimal gateway selection in sensor-cloud framework for health monitoring[J]. IET Wireless Sensor Systems, 2014, 4(2): 61-68.

[11] GERLA M, LEE E K, PAU G, et al. Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds[C]//2014 IEEE World Forum on Internet of Things (WF-IoT). 2014: 241-246.

[12] SIMMHAN Y, AMAN S, KUMBHARE A, et al. Cloud-based software platform for big data analytics in smart grids[J]. Computing in Science & Engineering, 2013, 15(4): 38-47.

[13] YURIYAMA M, KUSHIDA T. Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing[C]//13th International Conference on Network-Based Information Systems (NBiS).2010: 1-8.

[14] GE Y, ZHANG X, HAN B. Complex IoT control system modeling from perspectives of environment perception and information security[J]. Mobile Networks & Applications, 2017, 22(3):1-9.

[15] DIPIETRO R, GUARINO S, VERDE N V, et al. Security in wireless ad hoc networks-a survey[J]. Computer Communications, 2014, 51: 1-20.

[16] WANG T, PENG Z, WEN S, et al. Reliable wireless connections for fast-moving rail users based on a chained fog structure[J].Information Sciences, 2017, 379:160-176.

[17] WANG T, LI Y, WANG G J, et al. Sustainable and efficient data collection from WSN to cloud[J].IEEE Transactions on Sustainable Computing, 2017, PP(99):1-12.

[18] CHEN M, MA Y, LI Y, et al. Wearable 2.0: enabling human-cloud integration in next generation healthcare systems[J]. IEEE Communications Magazine, 2017, 55(1):54-61.

[19] MAN H A, YUEN T H, LIU J K, et al. A general framework for secure sharing of personal health records in cloud system[J]. Journal of Computer & System Sciences, 2017.

[20] CAI H, XU B, JIANG L, et al. IoT-based big data storage systems in cloud computing: Perspectives and challenges[J]. IEEE Internet of Things Journal, 2017, 4(1): 75-87.

[21] LIU J, SHEN S, YUE G, et al. A stochastic evolutionary coalition game model of secure and dependable virtual service in Sensor-Cloud[J]. Applied Soft Computing, 2015, 30(C):123-135.

[22] GARGEES R, MORAGO B, PELAPUR R, et al. Incident-supporting visual cloud computing utilizing software-defined networking[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2017, 27(1): 182-197.

[23] WANG T, LI Y, CHEN Y, et al. Fog-based evaluation approach for trustworthy communication in sensor-cloud system[J]. IEEE Communications Letters, 2017, 21(11): 2532-2535.

[24] WINKLER T, RINNER B. Security and privacy protection in visual sensor networks: a survey[J]. ACM Computing Surveys (CSUR), 2014, 47(1): 2.

[25] HE D, KUMAR N. A secure temporal credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks[J].Information Sciences, 2015, 321: 263-277.

[26] SAJID A, ABBAS H, SALEEM K. Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges[J]. IEEE Access, 2016, 4: 1375-1384.

[27] MARTIN K, WANG W. Aya: an efficient access-controlled storage and processing for cloud-based sensed data[C]//12th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). 2015: 130-134.

[28] SAHA S. Secure sensor data management model in a sensor-cloud integration environment[C]//Applications and Innovations in Mobile Computing (AIMoC). 2015: 158-163.

[29] ZHOU J, CAO Z, DONG X, et al. Security and privacy in cloud-assisted wireless wearable communications: challenges, solutions, and future directions[J]. IEEE Wireless Communications, 2015, 22(2): 136-144.

[30] HENZE M, HERMERSCHMIDT L, KERPEN D, et al. A comprehensive approach to privacy in the cloud-based internet of things[J]. Future Generation Computer Systems, 2016, 56: 701-718.

[31] BRUNEO D, DISTEFANO S, LONGO F, et al. IoT-cloud authorization and delegation mechanisms for ubiquitous sensing and actuation[C]//2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). 2016: 222-227.

[32] BUTUN I, MORGERA S D, SANKAR R. A survey of intrusion detection systems in wireless sensor networks[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 266-282.

[33] ALRAJEH N A, KHAN S, SHAMS B. Intrusion detection systems in wireless sensor networks: a review[J]. International Journal of Distributed Sensor Networks, 2013, 9(5): 167575.

[34] SMIRNOV A V, BORISENKO K A, SHOROV A V, et al. Network traffic processing module for infrastructure attacks detection in cloud

computing platforms[C]//2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM). 2016: 199-202.

[35] PATEL A, TAGHAVI M, BAKHTIYARI K, et al. An intrusion detection and prevention system in cloud computing: a systematic review[J]. Journal of Network and Computer Applications, 2013, 36(1): 25-41.

[36] SINHA N, PUJITHA K E, ALEX J S R. Xively based sensing and monitoring system for IoT[C]//International Conference on Computer Communication and Informatics (ICCCI). 2015: 1-6.

[37] RAY P P. A survey of IoT cloud platforms[J]. Future Computing and Informatics Journal, 2016, 1(1-2): 35-46.

[38] SUHAIL S, HONG C S, AHMAD Z U, et al. Introducing secure provenance in IoT: requirements and challenges[C]//International Workshop on Secure Internet of Things (SIoT). 2016: 39-46.

[39] DOUKAS C, MAGLOGIANNIS I. Bringing IoT and cloud computing towards pervasive healthcare[C]//Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). 2012: 922-926.

[40] PASHA S. ThingSpeak based sensing and monitoring system for IoT with Matlab Analysis[J]. International Journal of New Technology and Research (IJNTR), 2016, 2(6): 19-23.

[41] LOUNIS A, HADJIDJ A, BOUABDALLAH A, et al. Secure and scalable cloud-based architecture for e-health wireless sensor networks[C]//21st International Conference on Computer Communications and Networks (ICCCN). 2012: 1-7.

[42] BAEK J, VU Q H, LIU J K, et al. A secure cloud computing based framework for big data information management of smart grid[J]. IEEE Transactions on Cloud Computing, 2015, 3(2): 233-244.

[43] BUTUN I, EROL-KANTARCI M, KANTARCI B, et al. Cloud-centric multi-level authentication as a service for secure public safety device networks[J]. IEEE Communications Magazine, 2016, 54(4): 47-53.

[44] BUTUN I, WANG Y, LEE Y, et al. Intrusion prevention with two-level user authentication in heterogeneous wireless sensor networks[J]. International Journal of Security and Networks, 2012, 7(2): 107-121.

[45] BANAIE F, SENO S A H. A cloud-based architecture for secure and reliable service provisioning in wireless sensor network[C]//2014 4th International Conference on Computer and Knowledge Engineering (ICCKE).2014: 96-101.

[46] GOVINDAN K, MOHAPATRA P. Trust computations and trust dynamics in mobile ad hoc networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2012, 14(2): 279-298.

[47] JIANG J, HAN G, WANG F, et al. An efficient distributed trust model for wireless sensor networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2014, 26(5): 1.

[48] SAHA S, DAS R, DATTA S, et al. A cloud security framework for a data centric WSN application[C]//The 17th International Conference on Distributed Computing and Networking. 2016: 39.

[49] LOUNIS A, HADJIDJ A, BOUABDALLAH A, et al. Healing on the cloud: secure cloud architecture for medical wireless sensor networks[J]. Future Generation Computer Systems, 2016, 55: 266-277.

[50] ALBUQUERQUE S L, GONDIM P R L. Security in cloud-computing-based mobile health[J]. IT Professional, 2016, 18(3): 37-44.

[51] SHAH S H, KHAN F K, ALI W, et al. A new framework to integrate wireless sensor networks with cloud computing[C]//Aerospace Conference. 2013: 1-6.

[52] ZHU C, WANG H, LIU X, et al. A novel sensory data processing framework to integrate sensor networks with mobile cloud[J]. IEEE Systems Journal, 2016, 10(3): 1125-1136.

[53] PONMAGAL R S, DINESH N, RAJARAM U. Design and development of secure cloud architecture for sensor services[C]//International Conference on Distributed Computing and Internet Technology. 2015: 339-344.

[54] GUAN Z, YANG T, DU X, et al. Secure data access for wireless body sensor networks[C]//Wireless Communications and Networking Conference (WCNC). 2016: 1-6.

[55] HENZE M, HUMMEN R, MATZUTT R, et al. The sensorcloud protocol: securely outsourcing sensor data to the cloud[J]. arXiv preprint arXiv:1607.03239, 2016.

[56] GRANJAL J, MONTEIRO E, SILVA J S. Security in the integration of low-power wireless sensor networks with the internet: a survey[J]. Ad Hoc Networks, 2015, 24: 264-287.

[57] YUEN T H, ZHANG Y, YIU S M, et al. Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks[C]//European Symposium on Research in Computer Security. 2014: 130-147.

[58] MISRA S, SINGH A, CHATTERJEE S, et al. Mils-cloud: a sensor-cloud-based architecture for the integration of military tri-services operations and decision making[J]. IEEE Systems Journal, 2016, 10(2): 628-636.

[59] ZHU C, NICANFAR H, LEUNG V C M, et al. An authenticated trust and reputation calculation and management system for cloud and sensor networks integration[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(1):118-131.

[60] WHITEHEAD J R. Cluster-based trust proliferation and energy efficient data collection in unattended wireless sensor networks with mobile sinks[D]. Chattanooga: University of Tennessee. 2016.

[61] LUCA G D, CHEN Y. Visual IoT robotics programming language in pi-calculus[C]//International Symposium on Autonomous Decentralized System. 2017:23-30.

[62] LOMOTEY R K, PRY J C, CHAI C. Traceability and visual analytics for the Internet-of-Things (IoT) architecture[J]. World Wide Web-internet & Web Information Systems, 2017(4):1-26.

[63] GARGEES R, MORAGO B, PELAPUR R, et al. Incident-supporting visual cloud computing utilizing software-defined networking[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2017, 27(1): 182-197.

[64] ZHOU R, LAI Y, LIU Z, et al. A security authentication protocol for trusted domains in an autonomous decentralized system[J]. International Journal of Distributed Sensor Networks, 2016, 12(3): 5327949.

[65] YOON K, PARK D, YIM Y, et al. Security authentication system using encrypted channel on UAV network[C]//IEEE International Conference on Robotic Computing (IRC).2017: 393-398.

[66] ZHANG Y, LYU M R. QoS-aware byzantine fault tolerance[M]. QoS Prediction in Cloud and Service Computing. Singapore: Springor, 2017: 105-120.

[67] BHAT A, SAMII S, RAJKUMAR R. Practical task allocation for software fault-tolerance and its implementation in embedded automotive systems[C]//Real-Time and Embedded Technology and Applications Symposium (RTAS).2017: 87-98.

[68] ZHANG T, YAN L, YANG Y. Trust evaluation method for clustered wireless sensor networks based on cloud model[J]. Wireless Networks, 2016: 1-21.

[69] SUN D, ZHAO H, CHENG S. A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS[J]. Security and Communication Networks, 2016, 9(18): 5710-5723.

[70] LI X, HE J, ZHAO B, et al. A method for trust quantification in cloud computing environments[J]. International Journal of Distributed Sensor Networks, 2016, 12(2): 5052614.

[71] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the Internet of things[C]//Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. 2012: 13-16.

[72] TIAN W, ZHOU J Y, WANG G J, et al. Three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing[J]. IEEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1): 3-12.

[73] GARCIA LOPEZ P, MONTRESOR A, EPEMA D, et al. Edge-centric computing: vision and challenges[J]. ACM SIGCOMM Computer Communication Review, 2015, 45(5): 37-42.

[作者简介]

王田（1982-），男，湖南汨罗人，博士，华侨大学教授，主要研究方向为物联网及其安全问题、云计算技术、社交网络、软件安全、大数据处理等。

李洋（1991-），女，湖北黄石人，华侨大学硕士生，主要研究方向为传感云安全、雾计算、物联网等。

贾维嘉（1957-），男，中国香港人，博士，上海交通大学教授、博士生导师，主要研究方向为下一代无线通信、协议、异构网络等。

王国军（1970-），男，湖南长沙人，博士，广州大学教授、博士生导师，主要研究方向为网络和信息安全、物联网和云计算等。

彭绍亮（1979-），男，湖南长沙人，博士，国防科技大学教授，主要研究方向为分布式系统、计算机性能和无线网络等。