植入城市计算综述

李拴保[1,2,3] 傅建明[1,2] 连向磊[4]
(武汉大学计算机学院 武汉 430072)[1]
(武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)[2]
(河南财政税务高等专科学校 郑州 451464)[3] (中国人民解放军71155部队 潍坊 261000)[4]

摘 要 物联网通过感知技术实现物品与互联网的连接,云计算通过对共享资源的灵活整合和动态配置为用户提供面向需求的服务。基于上述背景,定义了植入城市计算的基本概念和功能框架,以植入城市计算应用场景为研究对象,比较了物联网技术与传统方法的数据采集、服务提供,论述了在人与环境交互中的感知应用部署、数据捕获、信息传播,阐述了云计算面向用户提供的数据管理服务、感知应用服务、位置查询服务。围绕植入城市计算的安全和隐私问题,对RFID隐私保护和身份认证、无线传感器网络密钥管理、参与感知隐私匿名化、云计算可信访问控制等进行了分析,并提出了进一步的研究方向。

关键词 物联网,云服务,参与感知
中图法分类号 TP393.08 **文献标识码** A

Survey on Embedded Urban Computing

LI Shuan-bao[1,2,3] FU Jian-ming[1,2] LIAN Xiang-lei[4]
(School of Computer, Wuhan University, Wuhan 430072, China)[1]
(Key Lab of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China)[2]
(Henan College of Finance and Taxation, Zhengzhou 451464, China)[3]
(71155 Troops of the Chinese People's Liberation Army, Weifang 261000, China)[4]

Abstract Internet of things realizes connecting of internet with anythings by sensing technology. Cloud computing provides requirement-oriented application service for users by sharing resources of flexible integration and dynamic configuration. The basic concept and function architecture was definited for embedded urban computing based on above-mentioned background. Taking application scenarios of embedded urban computing as the studying object, this paper compared data collecting and service provision between Internet of Things technology and traditional mode, dissertated sensing application deployment, data capturing, information spreading for human interacting with environment, elaborated user-oriented data management service, sensing application service, location query service provided by cloud computing, analyzed privacy protection and identity authentication for RFID, key management for wireless sensor network, privacy anonymized for participatory sensing, trusted access control for cloud computing around the security and privacy problem for embedded urban computing, proposed the future research direction.

Keywords Internet of things, Cloud service, Participatory sensing

1 引言

物联网是当前信息技术领域的热门话题,是产业界、学术界关注的焦点,它作为新兴技术在生产领域有着潜在的影响力。物联网涵盖经济、社会、技术多个方面含义,文献[1]从Things-Oriented、Internet-Oriented、Semantic-Oriented 3个视角诠释了物联网的概念、技术和标准;文献[2]从逻辑功能角度定义了物联网层次体系结构,从上层到底层依次包括应用层、中间件层、互联网层、访问网关层和边缘技术层;文献[3]从应用角度阐述了几种支撑技术:射频识别(Radio Frequency Identification,RFID)可以标识物品对象身份并读写身份数据,无线传感器网络(Wireless Sensor Networks,WSN)可以协作感知、采集、处理和传输网络覆盖地理区域内对象的监测信息,全球定位系统(Global Positioning System,GPS)可以提供导航服务。

我国城市化进程明显加快,大量物联网应用与城市公共服务发展密切相关。例如,RFID和NFC实时监控供应链的每一个环节[2];车载传感器网络提供车辆之间的距离数据,避

到稿日期:2012-10-01 返修日期:2012-12-10 本文受国家自然科学基金(61202387,90718005),河南省基础与前沿技术研究项目(122300410061),河南省软科学研究计划项目(122400450212)资助。
李拴保(1972-),男,博士生,主要研究方向为物联网、云计算、信息安全;傅建明(1969-),男,博士,教授,博士生导师,主要研究方向为可信计算、软件安全、网络安全。

免发生碰撞[3]；智能手机传感器记录周围环境状态[2]，根据汽车GPS数据判断路况拥堵[3]。城市空间部署了传感智能系统、移动设备和互联网应用，为我们提供了丰富的数据资源来感知城市的韵律，发掘城市中存在的隐患。如何协同利用这些数据，通过一个城市规模的计算来实现一个智慧、高效和绿色的城市，成为紧要研究课题。

当前环境催生了城市计算(Urban Computing)的理念：文献[4]提出了传感器应用于小规模的城市建筑环境，例如智能大厦；文献[5]提出了智慧城市的概念和应用领域，包括交通预报、城市设计、基于位置的服务；文献[6]提出，城市空间的任意设备、车辆、建筑、道路，包括人等都可作为一个计算单元，通过城市感知、数据挖掘、智能提取和服务提供这4个主要环节来建立一个城市级别的计算生态系统(如图1所示)，既为人们提供更美好的城市生活，又让城市本身变得更加绿色和智能。

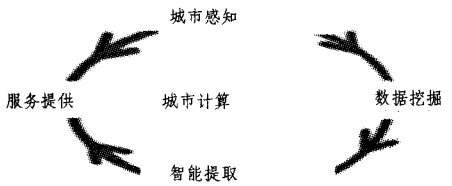

图1　城市计算的关键环节

城市计算若要低成本、可扩展、便利地提供服务，引入拥有丰富虚拟资源的云计算是当前的最佳选择。云计算是一个将大量计算资源、存储资源与软件资源链接在一起的共享虚拟IT资源池，以其便利、经济、高可扩展性等优势为广大远程用户访问服务。云计算[7]是一种模式，以最少的管理或交互代价，使无处不在、方便、按需网络访问可快速分配和释放可配置计算资源的共享池；云资源包括计算、应用、服务；云提供3种服务类型，即SaaS、PaaS和IaaS；共享数据存储云服务器，用户可随时随地访问服务。云计算作为新兴的基础设施，是提升城市公共服务水平、促进城市可持续发展的重要保障。物联网与云计算的关系密切[8]，物联网是面向特定领域和行业且拥有超量数据的复杂信息应用系统，云计算是实现物联网的一种软件解决方案。移动电话感知[50]和参与感知[9]的理念，进一步提出了参与感知城市应用模型。基于物联网、参与感知和云计算，研究城市感知及信息服务的提供，是一个非常重要的现实课题，基于上述背景提出了植入城市计算的基本概念和功能框架。

定义1　植入城市计算(Embedded Urban Computing)是指若干个物联网感知单元植入城市设施作为一个计算单元，协同完成数据采集、数据传输；个人参与感知城市设施关联的环境状态；由数据存储云计算服务平台为用户提供数据管理、感知应用、信息发布与查询服务。

植入城市计算功能框架(如图2所示)是感知、通信、服务功能的集合，包括城市感知层、通信网络层、云计算服务层。城市感知层是功能架构中的最底层，是城市设施计算单元中物联网感知和参与感知功能的集合；通信网络层是中继感知数据的无线通信网络基础设施的集合；云计算服务层是挖掘数据提供信息服务的集合。

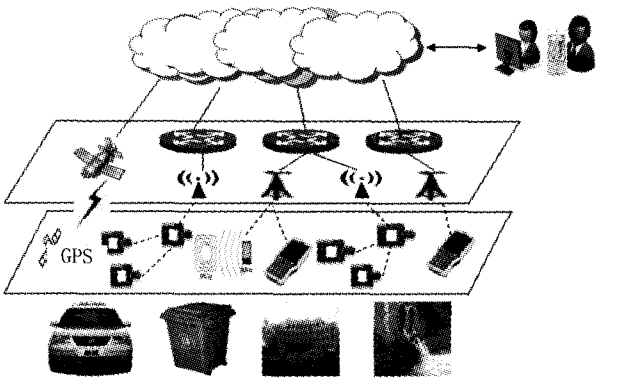

图2　植入城市计算功能框架

植入城市计算是一个感知、通信、服务分布不同层次结构的计算系统。本文以植入城市计算的应用场景为切入点，分析场景中采用物联网技术与传统方法的主要区别，阐述物联网、参与感知、云计算协同感知数据、提供服务的相关研究。第2节比较了垃圾处理、排污监测、交通监测3个应用场景中物联网技术与人工方法的不同；第3节分析参与感知在应用场景的具体应用和云计算提供应用场景的信息服务；第4节阐述物联网、参与感知、云计算存在的安全和隐私问题；最后总结全文。

2　植入城市计算应用场景

文献[2,3]提出了物联网在城市环境监测、交通物流领域的关键应用。垃圾处理、排污监测、交通监测等是物联网应用的一种场景，称为城市感知应用[9]。本节将说明物联网在场景中是如何实现的，相比传统方法解决了什么问题，从城市垃圾处理、排污监测、交通监测3个热点问题着手，详细阐述物联网应用的相关技术。

2.1　城市垃圾处理

随着城市化进程加快，城市垃圾侵占日益稀缺的土地资源。2010年环境统计年报[10]显示，全国城市垃圾堆放总量达70亿吨，占地75万亩。为了节约耕地、循环利用资源，垃圾分类回收、集中处理、产业化发展迫在眉睫。

现阶段垃圾处理的通常做法是：根据垃圾类别，将其投入不同特殊标记的垃圾筒；卡车定时回收垃圾筒，然后集中处理，成本高、效率低；人工统计月度年度分类处理总量，统计数据服务于业务管理，无法为政府管理决策和居民生活便利提供服务。垃圾处理不仅是政府责任，市民也希望参与进来；市民希望知道最近的垃圾箱分布位置以方便投放，当垃圾筒溢出时，个人可以向物业公司及时提供信息。政府决策需要相关数据：垃圾处理总量、卡车行驶路线。

物联网技术可以记录垃圾回收的全部过程，根据相关数据改进垃圾处理流程。例如，RFID标签应用于垃圾筒，标识其电子身份来统计可回收垃圾的数量[11]；RFID和GPS组合标识垃圾筒身份，以及定位卡车收集垃圾的运行轨迹[12]；RFID、GPS和GPRS实时记录数据以及废物产生的历史数据，计算卡车最佳行驶路线，实现最经济的垃圾回收模式[13]。相比传统方法，RFID系统实时统计分类垃圾回收总量、垃圾筒的GPS坐标，根据总量数据调整垃圾筒布局、坐标数据，安排卡车运行路线。但是，垃圾筒溢出时无法预先确定，个人通

过参与感知提供溢出信息。RFID 数据、GPS 坐标、参与感知信息存储于云计算服务平台，物业、个人、政府可以在任何时间、任何地点访问垃圾处理应用服务。

2.2 城市排污监测

随着城市化进程加快，城市排污量增多导致水系环境恶化。2010 年环境统计年报[10]显示，全国废水污水排放总量为 617 亿吨，化学需氧量排放总量为 1238 万吨。为了保护水系环境，废水污水净化处理后方可排入水体。

现阶段排污监测的通常做法是：人工定时采集污染源水质样本测试化学成份，运用统计方法对某时间段样本估计近似值，确定排污是否合格。这种方法样本数量有限，不能反映真实情况。环保部门通过媒体发布数据，为政府和居民提供参考。排污监测不仅是政府责任，市民也希望参与进来；市民希望了解小区附近污染源的影响，当出现新的污染源时，个人向环保部门及时提供信息。政府管理决策需要相关数据：污染源分布位置、排放时段、水质样本数据。

物联网技术可以自动采集污染源水质数据，消除了人工方法的非工作时间盲区。例如，大量化学传感器节点部署在污染源，节点数据通过无线传感器网络实时自动采集[14]；在水流湍急背景下，集成最新通信技术的无线传感器网络快速部署采集节点数据[15]。相比人工方法，WSN 网络连续采集样本数量充足、时间分布均匀，后台系统计算水质化学成份，准确度高；环保部门根据数据判定排污是否合格，个人参考数据安排生活。当出现新的污染源时，个人通过参与感知及时提供信息。污染源分布位置、排放时段、WSN 水质数据、参与感知信息存储于云计算服务平台，个人、政府可以在任何时间、任何地点访问排污监测应用服务。

2.3 城市交通监测

随着城市化进程加快，汽车数量急剧上升，导致交通事故恶化。2010 年交通事故统计年报[16]显示，全国道路交通事故造成 65225 人死亡，财产损失 9 亿。为了保护公民生命财产安全，监控汽车行驶速度迫在眉睫。

现阶段交通监测的通常做法是：在道路两侧安装测速型电子眼监测拍摄，根据测速数据计算平均值，判定汽车是否超速。这种方法只是被动限速，司机没有主动减速，不能避免交通事故。交通部门通过广播拥堵信息，为政府和个人提供参考。交通监测不仅是政府责任，市民也需要参与进来。个人了解出行区域车流分布、到达的畅通线路；当出现新的堵塞时，个人向交管部门及时提供信息。政府决策需要相关数据：堵塞区域车流分布、限速时段、交通流量。

物联网技术可以实现车辆与车辆、车辆与道路交互信息，司机会根据信息主动减速。例如，车载传感器网络可以在任何时间向邻近区域同向后方车辆即时发送紧急刹车信息，防止发生追尾事故[17]，车载多种传感器收集路面车辆密度、行人密度的感知信息[18]，十字路口车与车交互所处方位、运动速度和加速度[19]，可以达到安全限速的目标。相比传统方法，车与邻车直接获取限速信号可以避免碰撞，车流密度等数据可为政府管理参考。但是，现有方案传感器获得的数据只是反映车辆周围局部区域信息，而不能反映大范围连续区域的车流分布信息、交通流量信息。

鉴于文献[17,19]不能反映车流分布信息、交通流量信息，文献[20]提出了从车辆 GPS 系统记录的丰富轨迹数据可以发掘两个地点之间全天交通堵塞统计信息以及两地点之间所有可能的通路；从众多车辆的 GPS 轨迹数据可以计算出城市空间所有街道的交通流量、拥堵时段信息[21]，从而避免交通事故；车辆 GPS 系统和车载传感器协同计算出精确的车辆运行轨迹[22]，使得城市街道的车流分布预测信息更加准确。政府可以根据交通流量、拥堵时段和车流分布，动态调整城市街道车辆限速。

当突发性交通事故发生后，传感器和 GPS 系统计算的车流分布、交通流量不能反映道路的正常运行情况，个人通过参与感知及时提供信息。交通流量、拥堵时段、车流分布存储于云计算服务平台，个人、政府可以在任何时间、任何地点访问交通监测应用服务。

3 参与感知和云计算

参与感知推动了大量感知应用的发展，在植入城市计算的应用场景中，参与者可以部署环境感知应用，收集与应用场景关联的环境状态，实现人与环境的互动。云计算为政府决策和个人便利提供环境信息服务。

3.1 参与感知

通过智能手机部署的感知应用可以获得人与环境互动的状态信息。智能手机不仅可以作为计算和移动通信设备，而且嵌入丰富的传感器，使得可以部署面向个人、组织和社区的感知应用[50]。参与感知应用[9]的理念提出后，人可以是城市感知的参与者，利用智能手机可以随时随地收集环境状态、人与环境互动方式等数据。文献[51]定义了移动感知网络的概念，手机作为传感器网络节点，利用其感知硬件例如 GPS 芯片组、现代影像等能力访问网络基础设施；用户的自然分布性提供了数据收集的理想环境。无线传感器与移动电话无缝集成的协同感知网络体系架构[52]，满足感知应用要求的高质量和可用性。文献[32]提出了一种基于移动电话丰富功能和云计算服务的参与感知应用体系结构，包括移动数据捕获、数据存储和数据处理；移动感知应用捕获数据可以提交云服务处理，并与云服务交互处理结果。个人可以在智能手机部署面向环境的感知应用服务，记录垃圾处理、排污监测和交通监测的感知过程，获得更为丰富的环境状态数据，为政府决策和个人便利提供信息服务。

参与感知在不同环境中的数据捕获、信息传播差异较大。例如，1）近距离感知目标状态信息，在运动状态下一种移动电话传感器可以收集道路两边的设施信息[23]，利用移动电话嵌入的移动通信网络和短距离感知技术探测邻近区域目标对象的状态[24]。2）感知信息以互联网方式共享，移动电话物理传感器采集的数据以微博的形式分享给大家[25]。3）信息在一定感知网络内部传播，移动电话构建参与式静态摄像网络记录高速运动对象的状态[26]，移动电话传感器记录数据在移动电话呼叫合作传输中实现局部的信息共享[27]，移动电话传感器收集数据在无线传感器网络中传播[28]。目前，参与感知捕获内容有图片、位置、连接、信号处理等，移动电话构成的参与感知网络普遍存在，有效感知需要更多的普适移动电话和 Web 应用服务支撑。

总之，利用智能手机部署面向人与环境互动的参与感知应用，启动传感器工作；探测垃圾筒溢出状态，记录排污监测盲区水体影像，记录突发交通事故现场车流堵塞，定位垃圾

桶、监测盲区、事故现场 GPS 坐标，感知数据提交云计算服务平台，个人、政府访问云服务获得环境信息。

3.2 云计算

在植入城市计算应用场景中，垃圾处理、排污监测、交通监测的感知数据和个人参与的环境数据存储于云计算服务平台，云计算利用虚拟资源、低成本、可扩展、移动访问等优势，提供数据管理服务。同时，服务平台对感知数据统计分析深度挖掘，计算垃圾处理总量、污染源水体成份、区域交通流量等信息，提供感知应用服务。环境数据是城市感知应用的重要补充，服务平台统计区域垃圾筒分布、污染源分布、交通畅行线路，提供位置查询服务。

云计算是一种按需提供资源服务的计算模式，服务内容包括存储、计算、管理和应用服务，具有可靠性、安全性、可维护性、交互性等优势。云计算服务类型分为：基础设施即服务(Iaas)、平台即服务(Paas)、软件即服务(Saas)。

Iaas 是最底层服务[7,8]，为用户提供存储、网络以及其它资源方面的服务，用户根据需要部署操作系统和典型软件；典型服务有亚马逊的弹性云(Amazon, EC2)、Apache 的开源项目 Hadoop、谷歌的 Google compute engine。Paas 是构建于 Iaas 之上的服务[7,8]，为用户提供软件资源和开发语言，用户根据需要部署软件运行环境和配置；典型服务有谷歌的 Google app engine 和微软的 Microsoft Azure。Saas 是最顶层服务[7,8]，为用户提供定制的软件应用服务；典型服务有 Salesforce 公司的客户关系管理系统(CRM)和谷歌的在线办公软件。移动云计算[36]就是移动设备计算集中操作提交给云服务，包括搜索、数据挖掘和多媒体处理，移动终端接入云完成信息交互，例如 RIM 公司的黑莓企业电子邮件服务器、苹果的在线同步 MobileMe 服务、微软的数据同步 LiveMesh 服务、谷歌的 Android 系统平台和终端。

植入城市计算云服务平台提供 Saas 类型的数据管理服务、感知应用服务和位置查询服务。数据管理服务将感知数据、环境数据按照一定逻辑结构存储于云计算数据库系统，定时更新、删除、追加、查询；感知应用服务对数据统计分析，挖掘垃圾处理年度总量、卡车行驶主干线路、污染源总体分布、水质成份年度数据等政府决策所需信息；位置查询服务统计局部区域垃圾筒分布、排污监测盲区，参与者可以查询垃圾投放最近位置、已回收垃圾筒、最近污染源，发布垃圾筒溢出信息、新污染源位置。

在面向城市交通监测中，数据管理服务将车载传感器、GPS 数据、环境数据按照一定逻辑结构存储于云计算数据库系统，定时更新、删除、追加、查询；感知应用服务对数据统计分析，挖掘区域车流分布、道路交通流量、拥堵高峰时段等，政府可以依据信息预警堵塞线路，判定事故责任；位置查询服务统计公交站点分布、事故区域分布，参与者可以查询最近公交位置、最近出行线路，发布最新交通堵塞信息。

4 植入城市计算安全和隐私问题分析

植入城市计算功能体系存在攻击感知通信、信息服务的安全风险。在城市感知层，RFID 系统存在穷举攻击、窃听、隐私泄露[43]的风险；无线传感器网络节点之间存在密钥攻击、路由攻击、位置泄露的风险[54]；参与感知环境信息存在泄露参与者隐私、虚假参与信息[9]。在云计算服务层，存在云服务的非法越权访问、数据泄露[41,42]的风险。

4.1 RFID 安全和隐私

RFID 阅读器与标签通信，存在中间人攻击、中继攻击、穷举攻击、窃听，以及恶意阅读器记录标签对象踪迹、非授权访问标签内容的安全和隐私问题。

针对 RFID 标签隐私保护，一些文献提出标签内容加锁或签名的方法。标签内容哈希方法加锁[43]保护隐私，低运算量密码和基于身份签名[44]保护标签隐私，标签内容数字签名[45]响应阅读器指令来保护隐私。但是，若无认证，阅读器仍然可以扫描标签内部信息。

针对 RFID 系统身份认证，文献[55]提出了一种 AES 硬件加密 128 位数据块的对称挑战应答单项认证协议来实现标签认证阅读器，但其存在秘密密钥管理问题。文献[56]提出了一种基于 RSA 的认证方案，即标签内容被秘密密钥加密并且私钥签名后写入标签，在阅读器解密签名时认证校验，攻击者没有秘密密钥无法插入错误数据；这种方案无法区分伪造标签和认证的源标签。

基于伪造标签和恶意阅读器篡改标签内容的风险，文献[57]提出了一种基于共享密钥和随机数的双向认证和隐私保护安全协议，即阅读器与标签具有共享秘密密钥，阅读器与标签通过秘密密钥和随机数 SHA-1 哈希校验实现双向认证，标签隐私位由隐私状态变为非隐私状态，阅读器可以读取标签数据；但其存在秘密密钥存储空间问题。文献[58]提出了一种基于共享秘密值的双向认证安全协议，即 RFID 系统由标签、阅读器、后台服务器三方组成，标签与服务器共享标签身份和秘密值，阅读器与标签通过身份和秘密值 SHA-1 哈希检验实现双向认证，阅读器与服务器通过随机数和标签秘密值 SHA-1 哈希检验实现双向认证，以有效识别伪造标签和保护标签隐私。文献[57,58]利用哈希函数单向性增强了攻击复杂度，同时也增加了标签识别的计算复杂度；SHA-1 哈希函数的弱碰撞性[59]也暴露了认证协议的脆弱性。

许多领域使用移动 RFID 阅读器，此时，后台服务器与阅读器之间的无线通道处于非安全状态。文献[60]提出了面向后台系统与固定阅读器安全通道的相互认证和后台服务器与无线阅读器非安全通道的合作认证方案，即基于标签身份、阅读器身份、服务器与标签共享密钥、随机数、标签身份哈希匿名实现三方的相互认证，通过增加服务器与阅读器共享密钥、阅读器身份哈希匿名实现三方的合作认证。

RFID 系统安全和隐私的复杂性，使得认证和隐私保护的密钥管理异常复杂。单向认证无法识别伪造标签，双向认证阅读器与标签需要存储共享秘密密钥的额外空间，合作认证适合移动无线阅读器环境。上述研究是基于标签、阅读器、服务器不可信的背景，可信计算[31]是基于硬件安全模块支持下的可信计算平台，提供完整性校验服务，已经成功应用于微机系统和 PDA 系统。因此，作者提出可信阅读器背景下的身份认证和隐私保护。RFID 安全和隐私下一步研究的主要问题包括：RFID 近场超高频和超低能耗电路的实现；椭圆曲线(ECC)公钥密码在通信、安全上的优势；ECC 应用于阅读器和标签的单项认证；识别伪造标签和认证的源标签；可信移动阅读器背景下，服务器与标签的哈希匿名认证。

4.2 无线传感器网络安全

无线传感器网络节点之间的通信存在物理攻击、中间人

攻击、更改数据完整性、窃听消息、注入伪造数据，以及恶意传感器节点的路由攻击。

为了抵抗针对无线传感器网络的攻击，一些文献提出了传感器节点之间认证和数据加密的方法。基于轻量级对称密码和 HMAC 哈希函数组合[46]的传感器节点认证和数据加密，以及对称密码算法 CBC-MAC[47]传感器节点认证和数据加密，分散的密钥交换协议[61]抵制攻击者泄露节点，位置感知的密钥建立[62]抵制节点捕获攻击；但是，无密钥管理协议的认证、加密，使得传感器节点之间无法建立共同密钥的安全连接。

密钥管理协议是安全通信的核心，无线传感器网络密钥管理方案[63,64]分为 3 类：对称密钥管理、非对称密钥管理和混合密钥管理。

对称密码算法是对和运算，加解密速度快且易于硬件实现，一些文献提出了对称密钥预分发管理方案。每个传感器节点存储有预分发的主密钥[65]，另一传感器节点利用主密钥和随机数建立密钥对。每个传感器节点存储有一对预分发密钥[66]，用以迅速完成认证，但不适合大规模扩展。在静态传感器网络中，基于多项式池的一对预分发密钥[67]可以抵制节点泄露攻击。将完整二部图变为连接图的基于 Blom 矩阵的一对预分发密钥[68]可以抵制节点制造攻击，并且每个节点需要很少空间来存储密钥信息。基于二进制逻辑树的多空间 Blom 矩阵的一对预分发密钥[69]，弱化了 Blom 矩阵方案网络图的连通性，改进了攻击节点之间的妥协。对称 BIBD 预分发密钥[70]为每个传感器节点构造密钥链，相邻节点之间建立共享密钥实现安全通信。

公钥密码利用在密钥分配上的优势，建立密钥管理中心和密钥分配中心，负责密钥产生和分配。文献[71]提出了一种在外部实体和传感器网络之间的基于 RSA 的认证和密钥交换协议，外部实体提供签名的公钥和自己私钥签名的文本，传感器节点预装第三方 CA 分发的私钥，对随机数、消息校验和签名，与外部实体实现认证和密钥交换。文献[72]提出了基于 ECC 的 n-authentication 公钥认证方案，即用户可以对 n 个传感器节点之外的任意传感器子集进行认证。双线性映射下的基于 ID 的密钥协商[73]把身份字符串作为公钥加密，利用公共参数计算私钥，并将其分发给传感器节点，节点利用公共参数和私钥实现安全通信。基于非确定性多项式时间的 ID 密钥协商[74]，传感器节点所有参数应用于无线传感器网络生命周期内，参数包括大素数 p、加法群、乘法群、主密钥，传感器节点利用参数计算系统的公钥和私钥。

针对对称密码的低成本、高效率和非对称密码的密钥管理特性，文献[74]提出了无线传感器网络的混合密钥管理方案。由于传感器节点资源的限制，减少其高计算成本，密码运算负担在基站一边。

无线传感器网络的计算复杂性、通信复杂性、安全复杂性、规模扩展性，使得密钥管理异常复杂。对称密码管理方案相对低廉的计算复杂性，适合有限资源特性的无线传感器网络，但其安全性有限，不适合大规模场景。公钥密码在通信、安全、规模上有优势，但是对传感器网络来说计算成本太高。应降低密码计算量，设计适合嵌入式系统的轻量级密码算法；将可信计算应用于基站系统，降低计算成本。因此，作者提出可信基站背景的无线传感器网络密钥管理。无线传感器网络安全下一步研究的主要问题包括：无线传感器网络能源连续供应和超低能耗电路的实现，椭圆曲线密码密钥端、签名短、软件实现规模小、硬件实现电路省电的优势，以可信基站为中心，密码运算在基站一边，基站作为密钥分配中心与 n 个传感器节点集合单向认证。

4.3 参与感知隐私

参与感知实现人与环境的互动，云计算提供环境信息服务，感知过程存在恶意攻击者窃取参与者隐私、恶意参与者提供虚假信息的风险。文献[48]提出了参与感知应用中隐私信息的两个基本属性：时间和位置，保护参与者隐私信息免遭泄露的常见方法是隐私匿名化。文献[49]提出了基于恶意参与者贡献虚假数据的声誉成绩评价方法来评估虚假信息对云计算服务信誉的负面影响。

针对参与者隐私匿名化，文献[75]提出了一种保护位置隐私的匿名服务器，匿名服务器是一个可信第三方；参与者周期性向服务器提交自己的真实位置，服务器利用随机高斯噪声干扰算法输出参与者匿名位置，扰乱参数 μ 和 σ 来源于参与者历史访问记录，与参与者数量无关。文献[76]提出了一种与参与者数量相关的位置匿名混合微聚合方法，用户数量不大于门限值 k 时，采用 MT 匿名算法，而用户数大于 k 时，则采用微聚合 V-MDAV 匿名算法。匿名服务器体系简单，但是匿名服务器容易成为参与者输入信息的瓶颈。

为了消除匿名化的瓶颈作用，文献[77]提出了一种 MIX 匿名网络来匿名化参与者的报告时间、位置属性。MIX 定义了 L-多样性的时间空间匿名算法，时间、位置分成主属性、次属性，构造时间、位置的等价类并形成分组，LD-VMDAV 算法匿名主属性为一个值、次属性为 L 个值，匿名时间、位置报告应用服务器 AS，AS 无法泄露隐私信息。匿名网络保护参与者隐私在传播途径免遭泄露，但是无法防范恶意任务入侵参与者窃取隐私。文献[78]提出了一种从传播途径和恶意任务两方面保护参与者隐私的匿名方法，参与者通过 Tor 匿名网络下载任务防范攻击者窃取隐私，参与者报告含有时间、位置隐私信息的数字签名后通过 K-匿名服务发送，不含隐私信息组签名后通过 MIX 网络混淆路径发送。

匿名服务、匿名网络保护参与者隐私，需要外部实体共同完成，然而参与者自身没有匿名机制。文献[79]提出了一种匿名机制内化于参与者自身组件的参与感知应用通用系统模型，包含参与者、应用服务器、终端用户三方，参与者包含感知、处理、存储、报告 4 个组件，应用服务器包含任务、存储、处理、演示 4 个组件，每个组件均涉及隐私泄露问题。模型从任务、报告、存储、处理角度定义了每一组件处理隐私的方法：匿名任务发布给使用假名的参与者，避免记录参与者多次下载的时间和位置；参与者对任务剪裁感知避免泄露位置信息；隐私意识数据处理是参与者从原始数据移除敏感信息，避免泄露隐私；参与者用假名报告加密数据，避免泄露位置信息，报告数据隐藏敏感位置采用虚构位置痕迹产生；根据授权条件定义终端用户对感知数据的访问控制策略。参与感知通用模型体系简单，每个组件保护参与者自身隐私，但是无法防范恶意的参与者。文献[80]提出了利用周期伪随机和盲签名的面向参与感知应用的匿名声誉保护架构来阻止攻击者和参与者在多个假名之间建立连接，评估声誉积分，判定参与信息真伪。

参与感知隐私保护方案缤纷复杂，匿名服务方法可扩展性差，适合小规模参与者。匿名网络隔离参与者与恶意任务直接交互，限制感知应用的扩展。每个组件匿名化任务、报告、存储、处理，无法防范虚假信息。盲签名匿名声誉架构评估积分，没有隐私信息的量化标准。参与感知隐私保护需要进一步研究的问题包括：隐私可度量的方法与数据完整性的平衡，定制的系统性隐私保护方案与应用相互独立，隐私保护级别和标准的定义包括用户的反馈。

4.4 云服务安全

在公共云计算模式下，针对云服务的非法越权访问，必须通过非传统类访问控制手段实施可信访问控制。文献[42]提出基于密码学方法的可信访问控制来保证云服务的可用性，包括：分布式层次密钥的动态策略访问控制方案[81]、密钥策略的基于属性加密的细粒度访问控制方案[82]、密文策略的基于属性加密的属性撤销方案[83]、半可信代理公钥重加密方案[84]、组合代理重加密和 CP-ABE 的云环境下基于属性数据共享的属性撤销访问控制方案[85]，以及用户密钥或密文嵌入访问控制树的方案[37]。密码学方法面临的一个难点是用户权限撤销，一个基本方法是设置密钥生命周期[38]。文献[39]引入了用户授权列表；文献[40]提出基于用户的唯一 ID 属性及非门结构；文献[33]提出了多授权的 HABE 规模用户撤销方案，实现了私钥的全委托。

上述用户撤销方案都是针对数据对象的带有时间或约束的授权、访问控制，并且存在授权委托限制等亟待解决的问题。广播加密[29]实现没有时间等约束限制的用户撤销，文献[34]提出了基于用户身份的广播密文策略基于属性加密的撤销方案，减少了密文和私钥规模；文献[35]提出了具有最小私钥的广播加密撤销系统，密钥规模仅与椭圆曲线群元素个数相关，密文规模与撤销用户数量关联，提高了撤销效率；文献[30]首次提出 q-BDHE 条件下的串接广播和基于属性加密撤销方案：广播 cp-abe 和广播 kp-abe，具有直接撤销、共谋抵制和无连接多授权，实现用户身份、属性集、访问结构多重撤销机制，提高了效率。

云计算服务的低成本、便捷性、安全复杂性，使得可信访问控制的权限管理异常复杂。基于属性加密具有灵活细粒度访问控制特性，广播加密具有天然的撤销特性，密钥、密文规模与用户数量无关的特性，适合海量用户的云计算服务，但是需要维护一个撤销用户列表。上述权限撤销方法局限于用户特征，对于用户的具体权限：读、写、执行，没有详细研究。利用基于属性加密、广播加密的各自优点，构造具有撤销特性的密文策略基于属性加密方案；基于访问策略树构造非单调的权限树，树的叶子节点属性包含读、写、执行。因此，新方案中密文关联权限树，可以直接撤销用户的具体权限，使得以最小代价实现云服务的细粒度访问控制。

结束语 本文从物联网、云计算、参与感知在城市公共服务中应用的角度提出了植入城市计算的基本概念和功能框架。以植入城市计算应用场景为研究对象，研究了物联网技术在城市公共服务方面的应用部署，包括：①比较 RFID 系统与传统方法在城市垃圾处理中的数据采集、统计方式和服务对象；②分析无线传感器网络和人工方法在城市排污监测中的样本数量、统计方法和判定方式；③阐述传感器网络、GPS 系统与测速电子眼在城市交通监测中的信息交互、轨迹数据挖掘和交通流量计算；④针对个人与城市环境的互动，论述参与感知在智能手机中的感知应用部署、数据捕获方式和信息传播空间；⑤分析云计算数据管理的增、删、改，感知应用服务的统计分析、数据挖掘，面向用户的垃圾筒分布、交通站点分布查询服务；⑥围绕物联网、参与感知、云计算存在的安全和隐私风险，分析 RFID 系统的单向认证、双向认证、合作认证和标签隐私哈希匿名化，论述无线传感器网络对称密钥管理、非对称密钥管理和混合密钥管理，研究参与感知时间、位置隐私保护的匿名服务、匿名网络和匿名组件方法，阐述云计算分布式层次密钥、基于属性加密、代理重加密的可信访问控制和带有时间约束授权、基于广播加密的用户权限撤销。结合现有方案和可信计算、椭圆曲线密码的应用前景，展望了未来的研究方向。

参 考 文 献

[1] Atzori L, Iera A. The Internet of Things: A survey [J]. Computer Networks, 2010(54): 2787-2805

[2] Debasis B, Sen J. Internet of Things: Applications and Challenges in Technology and Standardization[J]. Wireless Pers Commun, 2011(58): 49-69

[3] 刘强，崔莉，陈海明. 物联网关键技术与应用[J]. 计算机科学，2010，37(6)：1-10

[4] Kindberg T, Chalmers M. Guest Editors introduction: Urban computing[J]. Pervasive computing, 2007, 6(3): 18-20

[5] Oliver N. Urban Computing and Smart Cities: Opportunities and Challenges in Modelling Large-Scale Aggregated Human Behavior[C]// HUB'11 Proceeding of the Second International Conference on Human Behavior Unterstanding. Berlin Heidelberg: Springer-Verlag, 2011: 16-17

[6] Zheng Yu, Liu Yan-chi, Yuan Jing, et al. Urban Computing with Taxicabs[C]// UbiComp'11. Beijing, 2011(09): 89-98

[7] Armbrust M, Fox A. Above the Clouds: A Berkeley View of Cloud Computing[R]. UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009

[8] 李乔，郑啸. 云计算研究现状综述[J]. 计算机科学，2011，38(4)：32-37

[9] Burke J, Estrin D, Hansen M. Participatory Sensing [C]// WSW'06 at SenSys'06. Boulder, Colorado, USA, October 2006

[10] http://zls.mep.gov.cn/hjtj/nb/2010tjnb

[11] Abdoli S. RFID application in municipal solid waste management system[J]. International Journal of Environment Research, 2009 (3): 447-454

[12] Hannana M A, Arebey M, Begum R A, et al, RFID and communication technologies for solid waste bin and truck monitoring system[J]. Waste Management, 2011, 31: 2406-2413

[13] Faccio M, Persona A, Zanin G. Waste collection multi objective model with real time traceability data[J]. Waste Management, 2011, 31: 2391-2405

[14] Capella J V, Bonastre A, Ors R. A Wireless Sensor Network approach for distributed in-line chemical analysis of water[J]. Talanta, 2010, 80: 1789-1798

[15] Sempere-Paya V M, Santonja-Climent. Integrated sensor and management system for urban waste water networks and prevention of critical situations[J]. Computers, Environment and Urban Systems, 2012, 36(1): 65-80

[16] http://www.moc.gov.cn/zhuzhan/tongjigongbao
[17] Tsugawa S. Inter-Vehicle communication and their applications tointelligent vehicles:an overview[C]//IEEE Intelligent vehicle symposium. 2002:564-569
[18] Li Zhi-heng, Li zhang-yi. IVS 09:Future research in vehicle vision systems[J]. IEEE Intelligent systems, 2009, 24(6):62-65
[19] Hung Chun-gen, Yarali A. Wireless services and intelligent vehicle transportation systems[C]//2011 24th Canadian Conference on Electrical and Computer Engineering(CCECE). 2011:63-68
[20] Song H J, Hsu H P, Yasan E, et al. New Approach to Predict the Quality of Service of Vehicle-Based GPS System in Mobile Environment[C]//Vehicular Technology Conference Fall(CTC 2009-Fall). 2009 IEEE 70th. HRL Labs., LLC, Malibu, CA, USA, Sept. 2009:1-5
[21] Zhu Lei, Bao Yuan-lu, Wang Sheng-Guo, et al. Map-Matching Compatible with Junction Adjusting in Vehicle Navigation System[C]//CSIE 2011, LNEE 129. 2011:451-457
[22] Jo K, Chu K, Sunwoo M. Interacting Multiple Model Filter-Based Sensor Fusion of GPS With In-Vehicle Sensors for Real-Time Vehicle Positioning[J]. IEEE Transactions on Intelligent Transportation Systems, 2012, 13(1)
[23] Hull B, Chen K, Zhang Yang, et al. Cartel:a distributed mobile sensor computing system[C]//4th ACM SenSys. 2006:125-138
[24] Frank C, Bolliger P, Mattern F, et al. The sensor internet at work:Locating everyday items using mobile phones[J]. Pervasive and Mobile Computing, 2008, 4:421-447
[25] Gaonkar S, Li J, Choudhury R R, et al. Micro-Blog:Sharing and Querying Content Through Mobile Phones and Social Participation[C]//Proc. ACM 6th International Conference on Mobile Systems, Applications, and Services. 2008:174-186
[26] Rege M R, Handziski V, Wolisz A. Using Participatory Camera Networks For Object Tracking[C]//2011 Fifth ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC). 2011:1-2
[27] Thiagarajan A, Biagioni J, Gerlich T, et al. Cooperative Transit Tracking using Smart-phones[C]//SenSys'10, Proceeding of the 8th ACM Conference on Embeded Networked Sensor System. November Zurich, Switzerland, 2010:85-98
[28] Jiao Wei-wei, Cheng Long, Chen Min. Efficient Data Delivery in Wireless Sensor Networks with Ubiquitous Mobile Data Collectors[C]//2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. 2010:232-239
[29] Fiat A, Naor M. Broadcast encryption [C]// Proc of Crypto 1993, volume 773 of LNCS. Springer-Verlag, 1993:480-491
[30] Attrapadung N, Imai H. Conjunctive Broadcast and Attribute-Based Encryption[J]. Pairing 2009, LNCS 5671. 2009:248-265
[31] 沈昌祥,张焕国,等. 信息安全综述[J]. 中国科学 E 辑:信息科学,2007,37(2):129-150
[32] Estrin D. Participatory Sensing:Applications and Architecture [J]. IEEE Internet Computing, 2010, 3:12-14
[33] Wang Guo-jun, Liu Qin, Wu Jie, et al. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. Computers & Security, 2011, 30:320-331
[34] Boneh D, Gentry C, Waters B. Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys[C]//Proceeding of Cryto'05, LNCS 3621. 2005:258-275
[35] Lewko A, Sahai A, Waters B. Revocation Systems with Very Small Private Keys[C]//2010 IEEE Symposium on Security and Privacy. 2010:273-285
[36] Liang Hong-bin, Huang Di-jiang, Peng Dai-yuan. On Economic Mobile Cloud Computing Model [C] // MOBICASE 2010, LNICST 76. 2012:329-341
[37] Hong Cheng, Zhang Min, Feng Deng-guo. AB-ACCS:A cryptographic access control scheme for cloud storage[J]. Journal of Computer Research and Development, 2010, 47(1):259-265
[38] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing[J]. SIAM Journal on Computing, 2003, 32(3):586-615
[39] Ibraimi L, Petkovic M, Nikova S, et al. Ciphertext-Policy attribute-based threshold decryption with flexible delegation and revocation of user attributes[R]. Technical Report. Centre for Telematics and Information Technology, University of Twente, 2009
[40] Roy S, Chuah M. Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs [R]. Technical Report. 2009
[41] Weber R H. Internet of Things - New security and privacy challenges[J]. computer law & security review, 2010, 26:23-30
[42] 冯登国,张敏,等. 云计算安全研究[J]. 软件学报,2011,22(1):71-83
[43] Weis S A. Security and Privacy in Radio-Frequency Id entification Devices[D]. Massachu settsInstitute of Technology, Cambridge, MA 02139, May 2003
[44] Calmels B, Canard S, Girault M, et al. Low-cost cryptography for privacy in RFID systems[C]//Proceedings of IFIP CARIDS 2006. Terragona, Spain, April 2006
[45] Juels A. RFID Security and Privacy: A Research Survey [J]. IEEE Journal on Selected Areas in Communications, 2006, 24 (2):381-394
[46] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C]//Proceedings of the Ninth ACM Conference on Computer and Communications Security. Washington, DC, USA, November 2002
[47] Gaubatz G, Kaps J-P, et al. Public key cryptography in sensor networks[C]//1st European Workshop on Security in Ad-hoc and Sensor Networks (ESAS 2004). 2004
[48] Debatin B, Lovejoy J P, Horn A K. Facebook and online privacy: attitudes, behaviors, and unintended consequences[J]. Journal of Computer-Mediated Communication, 2009, 15:83-108
[49] Huang K, Kanhere S, Hu W. Are You Contributing Trustworthy Data?: The Case for a Reputation System in Participatory Sensing[C]//Proc. of the 13th ACM International Conference on Modeling Analysis, and Simulation of Wireless and Mobile Systems (MSWiM). 2010:14-22
[50] Lane N D, Miluzzo E, Lu Hong, et al. A Survey of Mobile Phone Sensing[J]. IEEE Communications Magazine, 2010, 48(9):140-145
[51] Turner H, White J. Verification and Validation of Smartphone Sensor Networks[C]//Mobilware 2011, LNICST 93. 2012:233-247
[52] Zheng Ruan, Edith C-H, Ngai, et al. Wireless sensor deployment for collaborative sensing with mobile phones[J]. Computer Networks, 2011, 55:3224-3245

[53] Gandino F, Montrucchio B, Rebaudengo M. Tampering in RFID: A Survey on Risks and Defenses[J]. Mobile Netw Appl. ,2010, 15:502-516

[54] Tian Bin, Yang Yi-xian, Li Dong, et al. A security framework for wireless sensor networks[J]. The Journal of China Universities of Posts and Telecommunications, 2010, 17(Suppl. 2): 118-122

[55] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using AES algorithm[C]// Proceedings of Workshop on Cryptographic Hardware and Embedded Systems. Cambridge, MA, USA, August 2004

[56] Bernardi P, Gandino F, Lamberti F, et al. An anti-counterfeit mechanism for the application layer in low-cost RFID devices [C]// 4th European conference on circuits and systems for communications 2008 (ECCSC 2008). 2008: 227-231

[57] Liu A X, Bailey L A. PAP: A privacy and authentication protocol for passive RFID tags[J]. Computer Communications, 2009, 32: 1194-1199

[58] Cho J-S, Yeo S-S, Kim S K. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value[J]. Computer Communications, 2011, 34: 391-397

[59] Kapoor G, Piramuthu S. Vulnerabilities in Chen and Deng's RFID mutual authentication and privacy protection protocol[J]. Engineering Applications of Artificial Intelligence, 2011, 24: 1300-1302

[60] Doss R, Zhou Wan-lei, Sundaresan S. A minimum disclosure approach to authentication and privacy in RFID systems[J]. Computer Networks, 2012, 56: 3401-3416

[61] Wacker A, Knoll M, Heiber T, et al. A new approach for establishing pair wise keys for securing wireless sensor networks[C]// Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys). San Diego, CA, 2005

[62] Liu F, Rivera M, Cheng X. Location-aware key establish in wireless sensor networks [C] // Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC). Vancouver, Canada, 2006

[63] Camtepte S A, Yener B. Key distribution mechanisms for wireless sensor networks[R]. TR-05-07. 2005

[64] Boyle D, Newe T. Securing wireless sensor networks: security architectures[J]. Journal of Networks, 2008, 3(1): 65-77

[65] Zhu S, Setia S, Jajodia S. LEAP: efficient security mechanisms for large- scale distributed sensor networks[C]// Proceedings of the Tenth ACM Conference on Computer and Communications Security. October 2003: 62-72

[66] Chan H, Perrig A. Random key predistribution schemes for sensor networks[C]// Proceedings of the 2003 IEEE Symposium on Security and Privacy. May 2003: 197-213

[67] Liu D, Ning P. Improving key pre-distribution with deployment knowledge in static sensor networks[C]// ACM Transactions on Sensor Networks, 2005, 1(2): 204-239

[68] Du W, Deng J, Han Y, et al. A pairwise key pre-distribution scheme for wireless sensor networks[J]. ACM Transactions on Information and System Security (TISSEC), 2005, 8(2): 228-258

[69] Lee J, Stinson D R. Deterministic key predistribution schemes for distributed sensor networks[C]// Proceedings of ACM Symposium on Applied Computing 2004, Lecture notes in computer science, vol. 3357. Waterloo, Canada, 2004: 294-307

[70] Camtepe S A, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks [J]. IEEE/ACM Transactions on Networking(TON), 2007, 15(2): 346-358

[71] Watro R, Kong D, Cuti S, et al. Tinypk: securing sensor networks with public key technology[C]// Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks (SASN 04). New York, NY, USA: ACM Press, 2004: 59-64

[72] Ren K, Lou W, Zhang Y. Multi-user broadcast authentication in wireless sensor networks[C]// 4th Annual IEEE Communications Society Conference. 2007: 223-232

[73] Yang G, Rong C, Veigner C, et al. Identity-based key agreement and encryption for wireless sensor networks[J]. IJCSNS International Journal of Computer Science and Network Security, 2006, 6(5B): 182-189

[74] Zhang J, Varadharajan V. Group-based Wireless Sensor Network Security Scheme[C]// The fourth international conference on wireless and mobile communications (ICWMC 2008). July 2008

[75] Huang K L, Kanhere S S, Hu W. Towards privacy-sensitive participatory sensing[C]// Proceedings of the the 5th International Workshop on Sensor Networks and Systems for Pervasive Computing (PerSeNS 2009). TX, March 2009

[76] Solanas A, Martinez-Balleste A. V-MDAV: a multivariate microaggregation with variable group size[C]// 17th COMPSTAT Symposium of the IASC. Rome, 2006

[77] Huang K L, Kanhere S S, Hub W. Preserving privacy in participatory sensing systems[J]. Computer Communications, 2010, 33: 1266-1280

[78] Shin M, Cornelius C. AnonySense: A system for anonymous opportunistic sensing[J]. Pervasive and Mobile Computing, 2011, 7: 16-30

[79] Christin D, Reinhardt A. A survey on privacy in mobile participatory sensing applications [J]. The Journal of Systems and Software, 2011, 84: 1928-1946

[80] Christin D, Roßkopf C. IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications [C]// Proceedings of the IEEE Pervasive Computing and Communication. PerCom, 2012

[81] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control[C] // Guttan J, ed. Proc. of the 19th IEEE Computer Security Foundations Workshop—CSFW 2006. Venice: IEEE Computer Society Press, 2006: 5-7

[82] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proc. of CCS'06. 2006

[83] Bethencourt J, Sahai A, Waters B, et al. Ciphertext-Policy ABE [C]// Proceedings of the 28th IEEE Symposium on Security and Privacy(Oakland). 2007

[84] Blaze M, Bleumer G, Strauss M. Divertible Protocols and Atomic Proxy Cryptography[C] // Proc of EUROCRYPT 98. Espoo, Finland, 1998

[85] Yu Shu-cheng, Wang Cong, Lou Wen-jing, et al. Attribute Based Data Sharing with Attribute Revocation[C] // ASIACCS' 10. Beijing, China, 2010: 261-270