

信息交换过程中的隐私保护技术研究

华佳峰¹, 李凤华², 郭云川², 耿魁¹, 牛犇²

(1. 西安电子科技大学综合业务网理论与关键技术国家重点实验室, 陕西 西安 710071;
2. 中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093)

摘要: 结合国内外相关最新研究趋势, 对信息交换过程中的隐私保护问题进行了总结和展望。首先, 介绍了泛在网络中不同类型信息服务模式, 抽象信息传播的本质, 并分析了主体在信息流转过程中的隐私泄露风险; 其次, 总结归纳了环境信息的隐私感知、度量、隐私保护方案自适应调整、隐私分割与延伸授权的研究现状; 最后, 提出了多源环境信息的隐私感知、场景自适应的隐私度量、场景定义的隐私保护方案、隐私分割和延伸授权等4个未来研究方向。

关键词: 信息交换; 隐私保护; 隐私感知; 隐私分割; 延伸授权

中图分类号: TN929

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00035

Research on privacy protection in the process of information exchange

HUA Jia-feng¹, LI Feng-hua², GUO Yun-chuan², GENG Kui¹, NIU Ben²

(1. State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China;
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: The privacy preservation problems in the process of information exchange have been summarized, according to the latest study and review related. Firstly, the different kinds of information service modes in pervasive networks, induce the essence of the information dissemination were introduced, and the risks of privacy information leakage during the information exchange were analyzed. Then the current research status of the information privacy awareness, privacy metric, self-adaptive adjustment scheme, privacy splitting and authorization extension were concluded. Finally, four research directions including the privacy awareness in the multi-source environment, scenario-aware privacy measurement, scenario defined privacy protection scheme, privacy splitting and authorization extension were proposed.

Key words: information exchange, privacy preservation, privacy awareness, privacy splitting, authorization extension

收稿日期: 2016-02-07; 修回日期: 2016-03-02。通信作者: 牛犇, niuben@iie.ac.cn

基金项目: 国家自然科学基金—青年科学基金资助项目 (No.61502489); 国家高技术研究发展计划 (“863” 计划) 基金资助项目 (No.2015AA016007); 国家自然科学基金委—广东联合基金资助项目 (No.U1401251)

Foundation Items: The National Natural Science Foundation of China (No.61502489), The National High Technology R&D Program of China (863 Program) (No.2015AA016007), The Key Program of the National Natural Science Foundation of China-Guangdong Union Foundation (No.U1401251)

1 引言

网络技术、信息技术的持续快速发展和应用的广泛普及,推动形成了包含局域网、互联网、移动网和物联网等具有开放性、异构性、移动性、动态性、多安全域等诸多特性的泛在网络,其信息传播方式可以归纳为通过“网络之网络”访问“系统之系统”。泛在网络中,跨系统随机访问成为其信息交换的主体,为人们工作、生活、学习等提供了无限的便利。然而,此类访问会导致隐私信息在不同系统上的留存与交换,虽然该问题可以通过“等级保护”来实现不同等级的安全保护,但某一信息系统的泄露势必导致其他信息系统的隐私保护失效。因此,跨系统信息交换面临隐私信息泄露风险点多、动态隐私保护可控难等问题,隐私保护需求更加急迫。如图1所示,“人机物”借助泛在网络实现万物互联互通,以公共安全、智能交通、移动支付、智慧医疗、环境监测等为典型代表的泛在网络信息服务模式不断涌

现,信息的获取和利用在技术上已经达到“信息随心行、交互在指间”的信息传播理想境界。信息传播的实质是由若干个两两相连的信息系统动态随机连接,通过跨不同主管部门或单位的信息交换和共享,满足主体复杂的应用需求。在跨系统的信息交换过程中,面临的隐私问题遍及感知、匹配、度量、延伸授权等多个方面。面对这些威胁,泛在网络环境下的隐私保护机制需要全面地控制跨系统随机共享访问过程中用户隐私信息的泄露。信息频繁跨系统、跨安全域交换时,用户的隐私保护需求以及相应的隐私方案也将随时间、环境等因素动态变化,因此,隐私保护方案需加强普适性,以适应动态变化的时空场景和隐私需求;访问控制模型和访问策略也需适用于多信息系统和动态场景下的隐私信息管控,泛在网络环境下的隐私保护机制需要针对以上特征进行系统化研究,以有效减少跨系统信息交换过程中的隐私泄露风险和威胁,提升泛在网络信息可信可控传播技术水平。

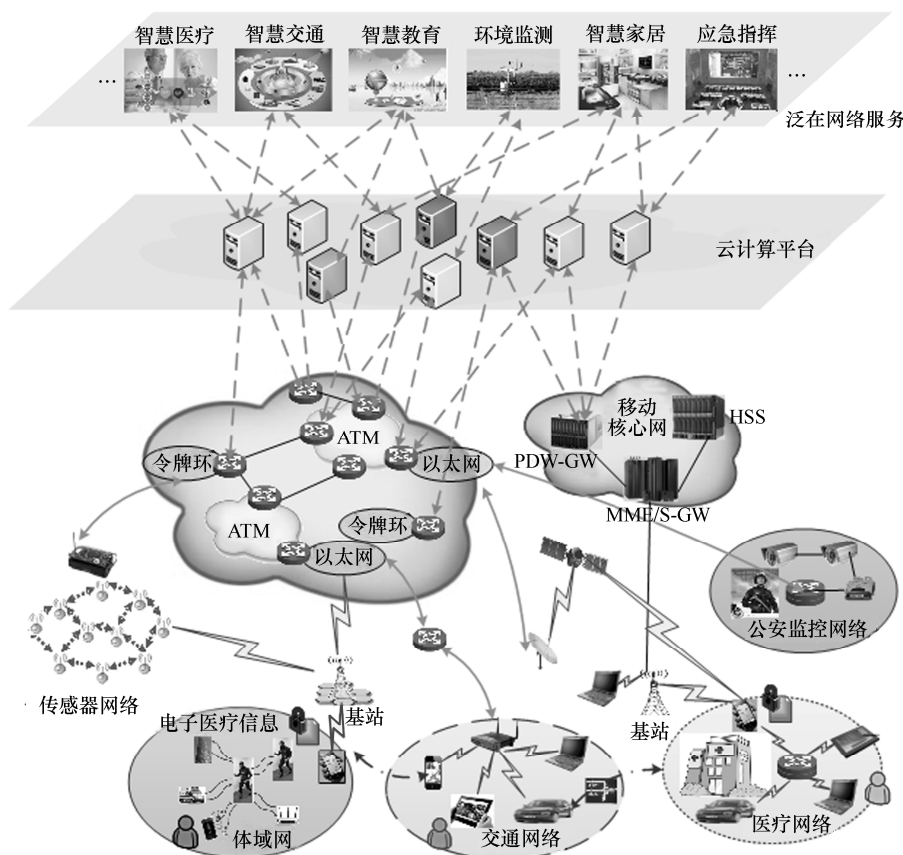


图1 万物互联促进信息的广泛共享

2 多源环境信息的隐私感知与动态度量机制研究进展

泛在网络跨系统信息交换过程面临的隐私问题遍及信息流转的各个环节,故本文拟从多源环境中的隐私感知、度量、隐私保护方案自适应调整、隐私分割与延伸授权这4个方面综述现有的隐私保护机制。

2.1 隐私感知的保护方案

大量文献对情景感知中的隐私保护问题进行了研究,Liu等^[1]提出了一种MAGPIE方案,该方案建立了各感知单元和隐私个体之间的信任关系,并利用混淆技术在保障数据可用性的同时,保证各个隐私个体的情景数据在共享的过程中不会被泄露。Li等^[2]提出了一种高效的Sum聚合协议,该协议采用加法同态加密和新型的密钥管理技术,支持大明文空间和最小时间序列数据集,并利用冗余技术对动态加入和离开的感知单元进行有效的隐私保护,有效地解决融合器不可信的问题,同时降低系统通信开销。在多维情景感知方面,Groat等^[3]提出了一种基于隐私保护的多维情景数据参与式感知方法,该方法采用NS(negative surveys)对多维情景数据进行分类,利用数据失真技术保护情景数据中的隐私信息,并推导出重建感知数据的原始概率密度函数。Qiu等^[4]提出了一种SLICER方案,首次利用 k -匿名保护技术实现对多个感知多媒体数据进行隐私保护,并利用聚合数据编码技术和消息传递策略,提出了数据传输策略TMU(transfer on meet up)和最低成本转移策略MCT(minimal cost transfer),有效保证多媒体数据的质量和隐私保护的效果。然而,这些方案大多专注于对参与感知的数据进行隐私保护,忽视了对关联数据进行融合分析带来的隐私泄露问题。

为此,Chakraborty等^[5]进一步研究多源情景数据关联分析带来的隐私泄露问题,从敌手的角度建立基于用户行为模式的推理函数,在此基础上计算情景数据融合后的隐私泄露概率。随后,Wang等^[6]假设恶意攻击者的攻击策略动态可调,将隐私感知策略视为用户和敌手的零和博弈,提出了极小极大学习算法以获得最优隐私保护策

略。Emiliano等^[7]提出了一种基于身份加密IBE(identity-based encryption)的隐私增强方案PEPSI(privacy-enhanced participatory sensing infrastructure),服务器利用简单的识别符来生成公钥对查询信息和感知信息的加解密,在整个过程中,不会泄露查询请求信息和感知信息,一定程度上满足了用户和感知单元的隐私需求。Wang等^[8]提出了一种ARTSense框架,利用匿名信誉管理协议和数据可信度评估方案,在对感知单元ID进行匿名的情况下,确定感知数据的可信度,同时满足了数据源的匿名和安全需求。Xing等^[9]提出了一种基于回归方法的隐私感知模型,该模型针对参与节点、集群和用户进行了一系列数据转换和聚合操作,并采用一种无需任何原始私有数据而准确表达知识意图的新方法进行回归拟合,能有效抵抗合谋攻击。

同时,面向医疗健康系统的隐私感知问题开始引起了广泛关注,Wang等^[10]设计了一个面向隐私保护的云辅助医疗监测系统,该系统利用压缩感知技术处理感知单元获得的稀疏数据、普通数据及带噪音数据,在保障感知数据准确性的同时,有效地降低传感网络的资源开销。Fredrikson等^[11]设计了一种新型的机器学习模型,该模型适用于医疗诊断和面部识别,利用预测置信度值进行反演攻击,这种新的攻击可以融合多源情景信息,从而实现用户意图的高效预测。

然而,目前大多数方案难以实现对多源环境数据隐私等级的细粒度感知。为此,Shin等^[12]提出了一种通用的隐私感知架构AnonySense,该架构对感知单元进行任务分配,即感知单元根据所感知信息的隐私等级,决定将该信息传送到不同的服务器中。Pallapa等^[13]进一步提出一种隐私量化方案,通过对情景感知系统中的每个感知单元分配隐私权重,并结合系统中的事务日志和情景状态,动态调整隐私保护策略,实现细粒度隐私保护普适环境下的情景感知系统。

此外,一些文献着重研究场景频繁变迁下的用户隐私需求感知。Simon等^[14]在隐私信息评估等相关研究工作中,建立了一个情景数据和到用户隐私之间的映射关系,通过感知动态环境信息,进而根据环境信息的变化调整用户对数据的访问

权限。Jana 等^[15]设计并实现了一种隐私保护系统 DARKLY，该系统通过集成计算机视觉库 OpenCV 部署多种隐私保护机制，包括访问控制、隐私保护算法和用户审计等，实现了环境感知下的隐私保护和服务质量之间的平衡。

综上，现有多数隐私信息感知方面的研究局限于单一场景或单一信息系统，欠缺对隐私需求会随时间、环境等因素动态变化的考虑，为了更好地在不同场景下为用户提供更加精准的隐私保护，需要结合用户所处环境、时空特征、历史行为等，对泛在网环境下的隐私信息和隐私需求进行细粒度感知。表 1 对相关工作进行了详细对比。

2.2 隐私度量方法

在位置服务隐私保护的相关领域，大量国内外研究工作者在隐私度量方面进行了深入研究。Assam 等^[16]研究地图匹配中的隐私保护问题，提出了一种基于马尔可夫模型的隐私位置匹配方案，该方案采用攻击者能够从发布的位置大数据中获取敏感位置的信息增益度量其隐私保护效果。Zheng 等^[18]提出了一个基于位置隐私保护的握手协议，利用布隆过滤器进行一对多的匹配，构建时空位置标记，并利用隐私信息泄露概率度量隐私保护效果。Wang 等^[19]提出了一种基于概率推测的位置大数据隐私保护技术，通过限制某一任意时刻 t 发布的位置数据所包含的信息量，利用概率推测的隐私保护技术假设攻击者具有全部背景知识，从而推测用户的隐私信息，进而对每个发布的位置数据计算其泄露风险，判断发布当前的位置数据是否违反用户的隐私需求，以定量地保护用户的位置隐私。此外，Yan 等^[20]关注无线传感器网络节点盗用带来的隐私保护风险，提出了一种基于组合框架的贝叶斯信任模型，该模型可有效评估节点的信任度。Goga 等^[21]提出了

一种隐私信息匹配方案的量化评估框架，并使用现实社交网络中采集的可靠数据进行仿真实验，评估准确度较高。

同时，由于泛在网络中各种类型的攻击威胁不断加剧，大量文献开始将攻击者的背景知识引入隐私度量的相关研究。Shokri 等^[22]提出了一种类属模型，假设敌手具有一定的背景知识和多种攻击手段，对攻击者的攻击方式进行形式化描述，设计一种位置隐私度量工具 Location-Privacy Meter，并利用现有的信息熵和 k -匿名等度量方式进行实际测试，测试结果达到预期。Wang 等^[23]提出了一种新型轨迹隐私度量方法，该度量方法将用户运动轨迹用带权无向图描述，并将攻击者的背景知识分级融入到度量方法中，基于信息熵计算用户的轨迹隐私水平。

此外，全局隐私度量逐渐成为国内外研究热点。Sun 等^[24]提出有障碍物的人工免疫聚类算法，根据免疫克隆优化亲和力函数计算障碍距离度量，并利用克隆选择原则，以精英抗体为基础更新聚类中心，实现全局最优聚类效果。Niu 等^[25,26]量化研究基于位置的隐私保护问题，从背景信息可能被敌手获取的问题入手，分析了这种潜在问题对隐私保护效果的影响，并提出了 2 种隐私度量函数，分别为基于信息熵的个人隐私度量函数和基于复用信息的全局隐私度量函数。然而，这些方案无法实现场景频繁变迁下的动态度量。Dahl 等^[27]对这一问题进行研究，提出了一种 CMIX 协议，对进入 Mix-Zone 内的车辆分配密钥并进行形式化描述，利用密码学方法对 Mix-Zone 隐私模型进行加密，运用推理方法实现对移动的隐私位置信息进行实时度量。为解决准标识符和隐私属性存在交叉难以划分的问题，Dwork 提出了“ ϵ -差分隐私”算法^[28,29]，该算法在数据集中

表 1

隐私感知相关工作对比

	隐私保护方法	是否基于可信第三方	密码方案	匿名	抗关联分析	抗合谋攻击
隐私感知	文献[1]	否	否	是	是	否
	文献[7]	是	是	否	否	否
	文献[8]	是	否	是	是	否
	文献[17]	否	是	否	否	是
	文献[14]	否	是	否	/	是

添加噪声,避免攻击者获得真实的数据。对数据集而言,添加一个数据不会对其统计特性造成影响,所产生的隐私泄露风险是极小的,即使攻击者具有一定背景知识,也无法通过观察查询结果而获得隐私信息,从而实现隐私保护效果。差分隐私的研究主要集中在如何添加冗余数据干扰分析结果,主要的技术包括针对整数类型数据的 Laplace 机制^[30]、针对浮点类型数据的 Exponential 机制^[31]以及它们在性能上的改进 Geometric 机制^[32]等。近几年,多种差分隐私保护模型相继出现被广泛地应用于数据挖掘领域的研究中^[33~36]。然而,目前差分隐私技术主要应用于离线数据的隐私保护,针对泛在网络中的动态应用场景的差分隐私保护方案少见报道。

综上,当前大多数隐私度量方法或模型针对静态的场景或单一模式上的隐私保护需求,忽略了泛在网络环境下时空属性、信任关系、环境信息等动态因素对隐私度量的影响,因此,需要根据实际应用,对不同环境下的不同运动对象的隐私进行实时动态度量。表2对相关工作进行了详细对比。

2.3 隐私保护方案自适应调整

大量文献对泛在网络环境下的隐私保护方案自适应调整进行研究,Yang 等^[39]提出了一种基于简单散列变化的隐私数据保护方法,对涉及用户隐私的文本数据进行深度挖掘,并利用隐私保护方案的自适应调整设计垃圾邮件过滤模型,能在一定程度上实现抗关联分析。Mao 等^[40]在基于可信第三方匿名服务器的基础上,提出一种情景自适应的位置隐私保护方法,当用户消费服务时,终端实时下载粗糙的路网情景数据,通过上下文

感知获取用户位置信息,进而实现系统自适应于用户个性化需求的隐私保护设置,并返回路网数据和查询结果,有效地降低了通信成本。

在基于位置的服务方面,Assam 等^[41]提出了一种新型隐私保护地图匹配技术,利用马尔可夫模型,基于位置隐私进行地图匹配,并引入新的成本函数来确定最短路径,有一定的实用性。Wang 等^[42]提出了一种面向个体的个性化扩展 1-多样性隐私匿名模型,该模型通过设置敏感属性的保护等级来实现隐私动态调整,并利用个性化扩展 1-多样性逆聚类算法实现隐私匿名。

在隐私信息匹配研究方面,Zhang 等^[43]在建立基于邻近的隐私信息匹配协议时考虑用户对不同兴趣的偏好程度,并利用 Paillier 同态加密方法设计不同等级的隐私保护方案。Li 等^[44]针对动态数据集的释放问题,利用新型距离抽样方法,提出 2 个解决方案,这些方案建立自适应调整反馈控制机制,获取数据集的动态阈值,为实现隐私数据的动态调整提供支持。

然而,这些方案大多是在静态场景下的自适应调整,缺乏灵活性,且普适性差。为此,Tian 等^[45]提出了一种可以根据兴趣点分布而自适应变化的 Hilbert 曲线(AHC),该曲线根据设定的存储容量将空间划分为原子区域,使用 Hilbert 曲线的分形规则确定各原子区域的顺序,并由此生成密钥树,数据拥有者可以将密钥树的一部分共享给授权使用者,从而实现对空间区域的自定义授权。Liu 等^[46]提出了一种新型自适应隐私保护策略,该策略具体建立了位置信息和使用者之间的映射关系,通过对不同类型信息进行标级,说明哪些信息能够在什么

表 2

隐私度量相关工作对比

度量方法	参考文献	优缺点	隐私保护判断标准
概率统计	文献[37] 文献[19]	原理简单,但计算复杂	概率越大,隐私泄露可能性越高
信息熵	文献[23] 文献[25]	实现简单	熵越大,隐私保护效果越好
差分隐私	文献[28] 文献[30] 文献[38]	容易实现,可满足所有查询类型,但噪声较大,查询次数有限	隐私保护预算越小,隐私保护水平越高

时候公布给哪些用户，一定程度上有效地解决了动态变化的位置隐私问题。

然而，大多数隐私保护等级自适应的相关措施不可避免导致高能耗的问题。因此，Mao 等^[47]提出了一种基于用户协作的自适应情景位置隐私保护方法，根据情景感知信息自主模糊个人真实位置，然后选择具有互助意愿的代理用户进行自适应的增量近邻查询，通过引入通信成本估算方法确定查询点位置，并采用 Voronoi 图技术过滤代理用户的查询结果，从而减少系统通信开销，有效地实现了位置隐私保护度与服务质量之间的平衡。Pallapa 等^[48]针对移动普适环境，提出了一种隐私混合方案，通过各个情景感知单元与环境之间的信息交互，实现了移动普适环境下的隐私保护方案自适应调整，同时降低资源消耗。

在隐私策略调整方面，Schaub 等^[49]提出了一种自适应的隐私保护模型，用户通过不断地与系统进行交互隐私认知，实现隐私策略的动态调整，系统将根据所处环境感知用户的隐私需求，从而实现隐私保护算法的自适应调整。随后，Schaub 等^[50]进一步提出了一种隐私决策模型，通过情景感知信息动态调整隐私决策模型中的隐私参数，以维持一个用户期望的隐私水平。Omoronyia 等^[51]提出了一种隐私保护策略自适应调整架构，通过感知场景和用户行为变化分析面临的隐私威胁，根据用户的隐私需求，动态调整与应用软件所分享的信息量。Wang 等^[52]关注隐私保护的长期效果，研究基于情境感知的 QoP (quality of protection) 机制，并开发出一种 QoP 框架，通过将两者结合起来利用情景感知技术实现服务质量与隐私保护的长期平衡，为移动网络中的用户提供个性化的隐私保护自适应服务。

综上，现有隐私保护方案在设计与实施过程

中往往会忽略动态性、频繁跨域迁移等需求，难以动态实时地保障用户在不同时间、多个场景之间频繁切换或使用多种服务应用时的隐私信息安全，尤其当敌手采用大数据关联分析攻击时，其成功率必然骤增。面对愈发多样化、个性化的用户需求，需要以实时满足用户的隐私保护需求为前提，为不同时空场景下的用户高效地提供隐私保护方案自适应调整。表 3 对相关工作进行了详细比对。

2.4 隐私分割与延伸授权的保护方案

泛在网络环境下，信息跨域频繁交换使信息在不同系统、不同安全域中留存，数据管理权和所有权的分离将导致数据安全和隐私泄露问题。针对这些现状，一些文献对隐私分割进行了研究。Itani 等^[54]提出了一种隐私即服务方案 PaaS (privacy as a service)，在基于可信第三方的基础上，对不同类型的数据进行分集，利用密码协处理器的防篡改能力，有效地实现了云服务器中隐私数据的安全存储、处理和审计。这种简单地通过加密将数据存储在服务器中的方法，在实际的数据操作过程中具有较大的开销，且容易引起单点失效攻击，隐私泄露风险大。Xu 等^[55]提出了一种基于数据分割与分级的云存储数据隐私保护机制，首先将数据合理分割为不同大小的数据块，再分别将小块数据和大块数据部署在本地和异地，然后按照数据本身不同的安全级别需求，采用联合数据染色和数据加密技术对隐私数据进行染色或加密，有效地保证了数据的安全性，同时提高系统灵活性并降低开销。Jiang 等^[56]提出了一个基于第三方租户数据安全保护模型，通过隐藏数据间的关系，利用数据分割技术对租户数据进行分级和切片，并利用单向函数混淆切片关系，结合租户对数据的隐私需求和安全等级定义，对

表 3 隐私保护方案自适应调整相关工作对比

隐私保护方法	隐私保护效果	资源消耗	服务质量
文献[49]	较强	适中	适中
文献[52]	较强	较大	较好
文献[51]	适中	适中	适中
文献[48]	较强	较大	适中
文献[53]	较强	适中	较好

租户数据进行分级,依据安全等级对分割后的子表内容进行局部加密或匿名,实现云端数据存储安全,为云计算提供有效的租户数据安全保护。Shi 等^[57]针对云计算安全和隐私保护问题,提出了一种基于数据分割的 CP-ABE (cipher text-policy attribute-based encryption) 隐私保护方案,利用数据分割策略对数据分割成不同的小数据块,通过 CP-ABE 算法进行加密,克服了云环境下第三方不可信的问题,在安全性和性能开销方面有一定的提升。

然而,这些方案无法适应泛在网络环境下信息跨域频繁交换过程中由于二次/多次转发、权限变更所带来的安全问题。在延伸授权方面,国外学者 Georgakakis 等^[58]提出了一种时间和位置感知的访问控制机制,该机制充分考虑访问时间、用户的移动性和位置信息,利用角色层次结构动态调整特殊情况下的访问控制策略,在提供传统的基于角色的访问控制的基础上,实现了紧急情况下的特殊访问。Tarameshloo 等^[59]提出了一种地理社会计算系统访问控制模型,该模型可以追踪用户当前位置,获得位置之间的初始空间关系,并通过初始空间关系的复合构造访问控制策略。Miettinen 等^[60]提出了一种场景感知的访问控制框架 ConXsense,该框架利用场景的安全属性和隐私属性等背景信息以及自适应、个性化的场景分类方法来实现场景感知的访问控制策略,避免了用户角色和访问控制策略的预定义,提供了准确和灵活的访问控制。Zhang 等^[61]基于 KP-ABE (key-policy attribute-based encryption) 提出了一种灵活高效的访问控制方案,该方案提供了灵活的用户关系机制,能够处理云计算环境下用户关系的频繁变化,可支持访问控制策略的逻辑表达和动态更改。Rubio-Medrano 等^[62]利用属性概念提出了一个面向协作网络环境的联合访问控制管理方案,该方案将本地上下文的属性信息映射为联合属性,实现跨组织资源共享访问,并建立了一整套属性生成规则和属性生成图,以及分布式环境下属性自动发现方法,实现了一定程度的柔性访问控制。Cappos 等^[63]针对智能手机的传感器隐私保护问题提出了一个动态、细粒

度的访问控制机制,该机制允许用户自定义和增加隐私过滤器,使用户能够将过滤后的数据公开给不可信的应用程序,也使研究人员能以一种保护用户隐私的方式收集数据开展研究。

国内学者 Wang 等^[64]提出使用线性秘密共享 (LSSS, linear secret sharing scheme) 矩阵块的方式来描述访问控制策略,使用 LSSS 矩阵块的 ABE (attribute-based encryption) 方案在计算量和通信方面具有轻量级、高效性、灵活性和安全性的优点,其可伸缩性为 ABE 机制提供了一个高效的策略管理平台。Zhou 等^[65]利用基于属性的签名验签技术,采用病人制定访问控制树来给医生授权的方式,提出了一个病人自主可控的、多级、提供隐私保护的联合授权机制,实现了分布式医疗云中 3 级的安全和隐私保护要求,并通过属性集合验证实现了直接授权医生、间接授权医生和其他人分类察看健康信息或者验证病人的身份。Zhang 等^[66]提出了一种面向空间索引树的访问控制模型,该模型建立了授权归类信息与索引树的关联,兼顾矢量数据与栅格数据等多种空间数据结构,并通过将空间授权信息添加到索引结构中,减少索引检索次数,提高了访问控制判断的效率。Liu 等^[67]针对云服务储存上的隐私问题,提出了隐私保护认证协议,该协议综合考虑匿名访问请求匹配机制的安全性和私密性实现访问权限的分配,采用基于属性加密算法实现用户只能访问自己的数据区,并利用代理重加密算法实现不同用户之间的数据共享。Wang 等^[68]基于属性加密算法提出了一种轻量级、安全的访问控制机制,该机制实现了多授权云中面向资源受限设备的轻量级、安全的数据访问控制机制,具有访问控制权限动态可伸缩的优点。Ma 等^[69]提出一个基于情景约束的柔性访问控制模型,该模型定义了基于情景约束的角色指派策略和角色授权策略,并给出策略集和角色分配与授权决策算法,支持“用户—角色”和“角色—权限”的自动指派,实现了工作流系统中基于情景的动态授权。Su 等^[70]以基于行为的访问控制模型为基础,提出了一种基于行为的多级安全访问控制模型,该模型将主体的安全等级、范畴扩展到行为上,通过行为映射函数实现主体在特定时间、特定地点访问行为

表 4

隐私分割与延伸授权相关工作对比

访问控制方法	密码方案	策略动态调整	控制粒度	场景感知能力	复杂度
文献[58]	否	是	粗	是	高
文献[61]	是	是	粗	否	高
文献[64]	是	是	细	否	低
文献[65]	是	是	细	否	高
文献[68]	是	是	粗	否	低
文献[70]	否	是	细	否	低

的安全属性获取，为授权策略的动态调整提供了支撑。Wu 等^[71]提出了一个基于属性的授权委托模型，该模型将权限的传递与权力的委托建立在实体所具有的属性集合的基础之上，以属性集合作为实体自身的代表进行授权，从而确保了拥有相同属性凭证链的各实体权限的一致性。表 4 对相关工作进行了详细比对。

3 结束语

本文首先分析了面向信息交换过程中隐私保护面临的威胁和挑战，然后从隐私感知、隐私度量、隐私保护方案自适应调整、隐私分割与延伸授权 4 个方面阐述分析了国内外最新研究动态。现有隐私保护方案大都解决单个信息系统或场景中的隐私保护问题，缺乏跨系统信息交换过程中的隐私保护，以及信息交换后的延伸授权。为了切实保护泛在网络环境中用户信息在频繁跨系统、跨网络、跨安全域交换时各个环节的隐私问题，还需要从以下几个方面进一步研究：1) 研究多源异构环境信息的形式化描述、隐私信息智能处理等方法或技术，分析情景数据中的时空变化规律，研究基于时空变化轨迹的隐私感知技术；2) 研究跨系统信息交换过程中的时空属性、信任关系、环境信息等因素对隐私度量的影响，从攻击者角度分析用户信息和行为被跟踪与被重构的可能性，利用信息熵、概率论等方法进行隐私的形式化描述和数学建模；3) 研究多参量自适应调节机制，通过对隐私保护算法中参数的合理调节，实现用有限算法适应多种场景的隐私保护目标；4) 研究面向网络空间的访问控制模型中各要素的属性信息，设计安全高效的属性描述机制，实

现柔性访问控制，解决跨系统信息交换的数据隐私分割与延伸授权问题。

参考文献：

- [1] LIU C G, JULIEN C. Pervasive context sharing in MAGPIE: adaptive trust-based privacy protection[J]. Mobile Computing, Applications, and Services, 2016, (162): 122-139.
- [2] LI Q H, CAO G H, PORTA T F L. Efficient and privacy-aware data aggregation in mobile sensing[J]. IEEE Transactions on Dependable and Secure Computing (TDSC), 2014, 11(2):115-129.
- [3] GROAT M M, EDWARDS B, HOREY J, et al. Enhancing privacy in participatory sensing applications with multidimensional data[J]. Pervasive & Mobile Computer, 2012, 9(5): 144-152.
- [4] QIU F D, WU F, CHEN G H. Privacy and quality preserving multimedia data aggregation for participatory sensing systems[J]. IEEE Transactions on Mobile Computing (TMC), 2015, 14(6): 1287-1300.
- [5] CHAKRABORTY S, RAGHAVAN K R, JOHNSON M P, et al. A framework for context-aware privacy of sensor data on mobile systems[C]//The 14th Workshop on Mobile Computing Systems and Applications. c2013:1-6.
- [6] WANG W, ZHANG Q. A stochastic game for privacy preserving context sensing on mobile phone[C]//IEEE International Conference on Computer Communications (INFOCOM). c2014: 2328-2336.
- [7] CRISTOFARO E D, SORIENTE C. PEPSI: privacy-enhanced participatory sensing infrastructure[C]//Communications of ACM. c2011: 23-28.
- [8] WANG X L, CHENG W, HAPATRA P M, et al. ARTSense: anonymous reputation and trust in participatory sensing[C]// IEEE International Conference on Computer Communications (INFOCOM). c2013: 2517-2525.
- [9] XING K, WAN Z G, HU P F, et al. Mutual privacy-preserving regression modeling in participatory sensing[C]//IEEE International Conference on Computer Communications (INFOCOM). c2013: 3039-3047.
- [10] WANG C, ZHANG B S, REN K, et al. A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing[C]//

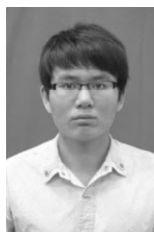
- IEEE International Conference on Computer Communications (INFOCOM). c2014: 2130-2138.
- [11] FREDRIKSON M, JHA S, RISTENPART T. Model inversion attacks that exploit confidence information and basic countermeasures[C]//The 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS). c2015: 1322-1333.
- [12] SHIN M, CORNELIUS C, PEEBLES D, et al. AnonySense: a system for anonymous opportunistic sensing[J]. *Pervasive and Mobile Computing*, 2011, 7(1): 16-30.
- [13] PALLAPA G, ROY N, DAS S K. A scheme for quantizing privacy in context-aware ubiquitous computing[C]//The 4th International Conference on Intelligent Environments. c2008: 1-8.
- [14] SIMON M, SVETHA V, GEOFF. Dynamic privacy assessment in a smart house environment using multimodal sensing[J]. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 2008, 5(2): 1-29.
- [15] JANA S, NARAYANAN A, SHMATIKOV V. A scanner darkly: protecting user privacy from perceptual applications[C]//IEEE Symposium on Security and Privacy (S&P). c2013: 349-363.
- [16] ASSAM R, SEIDL T. Private map matching: realistic private route cognition on road networks[C]//IEEE 10th International Conference on Ubiquitous Intelligence and Computing, Autonomic and Trusted Computing (UIC/ATC). c2013: 178-185.
- [17] CRISTOFARO E D, SORIENTE C. Participatory privacy: enabling privacy in participatory sensing[J]. *IEEE Network*, 2013, 27(1): 32-36.
- [18] ZHENG Y, LI M, LOU W, et al. Location based handshake and private proximity test with location tags[J]. *IEEE Transactions on Dependable and Secure Computing*, 2015: 1.
- [19] 王璐, 孟小峰. 位置大数据隐私保护研究综述[J]. *软件学报*, 2014, 25(4): 693-712.
- WANG L, MENG X F. Location privacy preservation in big data era: a survey[J]. *Journal of Software*, 2014, 25(4): 693-712.
- [20] 鄢旭, 陈晶, 杜瑞颖, 等. 无线传感器网络中基于组合框架的贝叶斯信任模型[J]. *计算机应用研究*, 2012, 29(3): 1078-1083.
- YAN X, CHEN J, DU R Y, et al. Bayes trust model based on combinatorial frame in WSNs[J]. *Application Research of Computers*, 2012, 29(3): 1078-1083.
- [21] GOGA O, LOISEAU P, SOMMER R, et al. On the reliability of profile matching across large online social networks[C]//ACM Sigkdd International Conference on Knowledge Discovery and Data Mining. c2015: 1799-1808.
- [22] SHOKRI R, THEDODORAKOULOS G, DANEZIS G, et al. Quantifying location privacy: the case of sporadic location exposure[C]//The 11th International Symposium on Privacy Enhancing Technologies. c2011: 57-76.
- [23] 王彩梅, 郭亚军, 郭艳华. 位置服务中用户轨迹的隐私度量[J]. *软件学报*, 2012, 23(2): 352-360.
- WANG C M, GUO Y J, GUO Y H. Privacy metric for user's trajectory in location-based services[J]. *Journal of Software*, 2012, 23(2): 352-360.
- [24] SUN L, LUO Y, DING X, et al. A novel artificial immune algorithm for spatial clustering with obstacle constraint and its applications[J]. *ACM Computational Intelligence and Neuroscience*, 2014, 2014(13): 1-11.
- [25] NIU B, LI Q, ZHU X, CAO G, et al. Achieving k-anonymity in privacy-aware location-based services[C]//IEEE International Conference on Computer Communications(INFOCOM).c2014: 754-762.
- [26] NIU B, LI Q, ZHU X, CAO G, et al. Enhancing privacy through caching in location-based Services[C]//IEEE International Conference on Computer Communications(INFOCOM).c2015: 1017-1025
- [27] DAHL M, DELAUNE S, STEEL G. Formal analysis of privacy for vehicular mix-zones[C]//The 15th European Symposium on Research in Computer Security. c2010: 55-70.
- [28] DWORK C. Differential privacy: a survey of results[C]//The 5th International Conference on Theory and Applications of Models of Computation (TAMC). c2008: 1-19.
- [29] DWORK C. Ask a better question, get a better answer: a new approach to private data analysis[C]//The 11th International Conference on Database Theory (ICDT'07). c2007: 18-27.
- [30] DWORK C. Differential privacy[C]//The 33rd International Colloquium of the Automata, Languages and Programming(ICALP'06). c2006, 26(2): 1-12.
- [31] MCSHERRY F, TALWAR K. Mechanism design via differential privacy[C]//The 48th Annual IEEE Symposium on Foundations of Computer Science(FOCS'07). c2007: 94-103.
- [32] GHOSH A, ROUGHGARDEN T, SUNDARARAJAN M. Universally utility-maximizing privacy mechanisms[J]. *SIAM Journal on Computing*, 2012, 41(6): 1673-1693.
- [33] BLOCKI J, BLUMAND A, DATTA A, et al. The Johnson-Lindenstrauss transform itself preserves differential privacy[C]//The 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science(FOCS'12). c2012: 410-419.
- [34] BONOMI L, XIONG L, CHEN R, et al. Frequent grams based embedding for privacy preserving record linkage[C]//The 21st ACM International Conference on Information and Knowledge Management. Hawaii. c2012: 1597-1601.
- [35] FANAND L, XIONG L. Real-time aggregate monitoring with differential privacy[C]//The 21st ACM International Conference on Information and Knowledge Management. Hawaii, c2012. 2169-2173.
- [36] CHEN J, NAUGHTON J F, CAI J Y. On differentially private frequent itemset mining[J]. *The International Journal on Very Large Data Bases*, 2012, 6(1): 25-36.
- [37] LU R X, LIN X D H, LUAN T, et al. Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2012, 61(1): 86-96.
- [38] 熊平, 朱天清, 王晓峰. 差分隐私保护及其应用[J]. *计算机学报*, 2014, 37(1): 101-122.
- XIONG P, ZHU T Q, WANG X F. A survey on differential privacy and applications[J]. *Chinese Journal of Computers*, 2014, 37(1): 101-122.
- [39] 杨震, 范科峰, 雷建军. 隐私保护的自适应垃圾邮件过滤方法研

- 究[J].通信学报, 2009, 30(51): 145-149.
- YANG Z, FAN K F, LEI J J. Privacy preserving online spam filtering[J]. Journal on Communications, 2009, 30(51): 145-149.
- [40] 毛典辉, 蔡强, 李海生, 等. 一种自适应情景的位置隐私保护方法[J]. 中南大学学报(自然科学版), 2013, 44(S2): 279-283.
- MAO D H, CAI Q, LI H S, et al. An adaptive context-aware location privacy protection method[J]. Journal of Central South University (Science and Technology), 2013, 44(S2): 279-283.
- [41] ASSAM R, SEIDL T. Private map matching: realistic private route cognition on road networks[C]//The 10th IEEE International Conference on Ubiquitous Intelligence and Computing, and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC'13). c2013:178-185.
- [42] 王波, 杨静. 一种基于逆聚类的个性化隐私匿名方法[J]. 电子学报, 2012, 40(5): 883-890.
- WANG B, YANG J. A personalized privacy anonymous method based on inverse clustering[J]. Acta Electronica Sinica, 2012, 40(5): 883-890.
- [43] ZHANG R, ZHANG J, ZHANG Y, et al. Privacy-preserving profile matching for proximity-based mobile social networking[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 656-668.
- [44] LI H, XIONG L, JIANG X Q, et al. Differentially private histogram publication for dynamic datasets: an adaptive sampling approach[C]//The 24th ACM International on Conference on Information and Knowledge Management, Melbourne. c2015: 1001-1010.
- [45] 田丰, 桂小林, 张学军, 等. 基于兴趣点分布的外包空间数据隐私保护方法[J]. 计算机学报, 2014, 37(1): 123-138.
- TIAN F, GUI X L, ZHANG X J, et al. Privacy-preserving approach for outsourced spatial data based on POI distribution[J]. Chinese Journal of Computers, 2014, 37(1): 123-138.
- [46] 刘昭斌, 刘文芝, 顾君忠. 位置感知的自适应隐私保护策略[J]. 计算机工程与设计, 2011, 32(3): 839-841, 1032.
- LIU Z B, LIU W Z, GU J Z. Adaptive privacy protection policy of location-aware[J]. Computer Engineering and Design, 2011, 32(3): 839-841, 1032.
- [47] 毛典辉, 蔡强, 李海生, 等. 用户协作模式下自适应情景的 LBS 隐私保护方法[J]. 四川大学学报(工程科学版), 2013, 45(4): 124-130.
- MAO D H, CAI Q, LI H S, et al. An adaptive context-aware LBS privacy protection method based on users collaboration[J]. Journal of Sichuan University (Engineering Science Edition), 2013, 45(4): 124-130.
- [48] PALLAPA G, DAS S K, FRANCECO M D, et al. Adaptive and context-aware privacy preservation exploiting user interactions in smart environments[J]. Pervasive and Mobile Computing, 2014, 12(11): 232-243.
- [49] SCHAUB F, KONINGS B, WEBER M, et al. Towards context adaptive privacy decisions in ubiquitous computing[C]// The 9th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops'12). c2012: 407-410.
- [50] SCHAUB F, KONINGS B, LANG P, et al. PriCal: context-adaptive privacy in ambient calendar displays[C]//The 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'14). Seattle, c2014: 499-510.
- [51] OMORONYIA I, CAVALLARO L, SALEHIE M, et al. Engineering adaptive privacy: on the role of privacy awareness requirements[C]//The 35th IEEE International Conference on Software Engineering (ICSE'13). c2013: 632-641.
- [52] WANG W, ZHANG Q. Toward long-term quality of protection in mobile networks: a context-aware perspective[J]. IEEE Wireless Communications, 2015, 22(4): 34-40.
- [53] ZHANG K, YANG K, LIANG X H, et al. Security and privacy for mobile healthcare networks: from a quality of protection perspective[J]. IEEE Wireless Communications, 2015, 22(4): 104-112.
- [54] ITANI W, KAYSSI A, CHEHAB A. Privacy as a service: privacy-aware data storage and processing in cloud computing architectures[C]//The 8th International Conference on Dependable, Autonomic and Secure Computing (DASC'09). Chengdu. c2009: 711-716.
- [55] 徐小龙, 周静岚, 杨庚. 一种基于数据分割与分级的云存储数据隐私保护机制[J]. 计算机科学, 2013, 40(2): 98-102.
- XU X L, ZHOU J L, YANG G. Data privacy protection mechanism for cloud storage based on data partition and classification[J]. Computer Science, 2013, 40(2): 98-102.
- [56] 江颀, 顾祝燕, 高骏骁, 等. 基于敏感等级的云租户数据安全保护模型研究[J]. 系统工程理论与实践, 2014, 34(9): 2392-2401.
- JIANG J, GU Z Y, GAO J X, et al. Cloud tenants-oriented data security protection model based on data sensitivity grading[J]. Systems Engineering Theory & Practice, 2014, 34(9): 2392-2401.
- [57] 施荣华, 刘鑫, 董健, 等. 云环境下一种基于数据分割的 CP-ABE 隐私保护方案[J]. 计算机应用研究, 2015, 32(2): 522-523, 527.
- SHI R H, LIU X, DONG J, et al. Privacy protection scheme in cloud computing using CP-ABE based on data partition[J]. Application Research of Computers, 2015, 32(2): 521-523, 527.
- [58] GEORGAKAKIS E, NIKOLIDAKIS S A, VERGADOS D D, et al. Spatio temporal emergency role based access control (STEM-RBAC): a time and location aware role based access control model with a break the glass mechanism[C]//The 16th IEEE International Symposium on Computers and Communications (ISCC'11). c2011: 764-770.
- [59] TARAMESHLOO E, FONG P W L. Access control models for geo-social computing systems[C]//The 20th ACM Symposium on Access Control Models and Technologies (SACMAT'14). London, c2014: 115-126.
- [60] MIETTINEN M, HEUSER S, KRONZ W, et al. ConXsense: automated context classification for context-aware access control[C]//The 9th ACM Symposium on Information, Computer and Communications Security (CCS'14). Kyoto, c2014: 293-304.
- [61] ZHANG Y, CHEN J, DU R, et al. FEACS: a flexible and efficient access control scheme for cloud computing[C]//The 13th IEEE In-

ternational Conference on Trust, Security and Privacy in Computing and Communications (TRUSTCOM'14). Beijing, c2014: 310-319.

- [62] RUBIO-MEDRANO C E, ZHAO Z, DOUPE A, et al. Federated access management for collaborative network environments: framework and case study[C]//The 20th ACM Symposium on Access Control Models and Technologies (SACMAT'15). c2015: 125-134.
- [63] CAPPOS J, WANG L, WEISS R, et al. BlurSense: dynamic fine-grained access control for smartphone privacy[C]//The IEEE Sensors Applications Symposium (SAS'14). c2014: 329-332.
- [64] WANG J, HUANG C, WANG J. Scalable access policy for attribute based encryption in cloud storage[M]//Algorithms and Architectures for Parallel Processing. Berlin: Springer, 2015: 383-402.
- [65] ZHOU J, LIN X D, DONG X L, et al. PSMIPA: patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system[J]. IEEE Transactions on Parallel & Distributed Systems, 2015, 26(6):1693-1703.
- [66] 张颖君,冯登国,陈恺.面向空间索引树的授权机制[J].通信学报,2010, 31(9):64-73.
ZHANG Y J, FENG D G, CHEN K. Authorization mechanism based on spatial index[J]. Journal on Communications, 2010, 31(9): 64-73.
- [67] LIU H, NING H S, XIONG Q X, et al. Shared authority based privacy-preserving authentication protocol in cloud computing[J]. IEEE Transactions on Parallel & Distributed Systems, 2015, 26(1):241-251.
- [68] WANG Y C, LI F H, XIONG J B, et al. Achieving lightweight and secure access control in multi-authority cloud[C]//The 2015 IEEE Trustcom/BigDataSE/ISPA. c2015: 459-466.
- [69] 马晨华, 王进, 裘昊, 等. 基于情景约束的工作流柔性访问控制模型[J]. 浙江大学学报(工学版), 2010, 44(12): 2297-2308.
MA C H, WANG J, QIU J, et al. Flexible context-constraint-based access control model for workflows[J]. Journal of Zhejiang University (Engineering Science), 2010, 44(12): 2297-2308.
- [70] SU M, LI F H, TANG Z, et al. An action-based fine-grained access control mechanism for structured documents and its application[J]. The Scientific World Journal, 2014: 232708-232720.
- [71] 吴彬, 冯登国. 多域环境下基于属性的授权委托模型[J]. 软件学报, 2011, 22(7): 1661-1675.
WU B, FENG D G. Attribute-based authorization delegation model in multi-domain environments[J]. Journal of Software, 2011, 22(7):1661-1675.

作者简介:



华佳烽 (1989-), 男, 湖北黄冈人, 西安电子科技大学博士生, 主要研究方向为信息安全、隐私保护。



李凤华 (1966-), 男, 湖北浠水人, 博士, 中国科学院信息工程研究所副总工、研究员、博士生导师, 主要研究方向为网络与系统安全、隐私计算、信息保护。



郭云川 (1977-), 男, 四川营山人, 博士, 中国科学院信息工程研究所副研究员, 主要研究方向为物联网安全、形式化方法。



耿魁 (1989-), 男, 湖北红安人, 西安电子科技大学博士生, 主要研究方向为网络安全。



牛犇 (1984-), 男, 陕西西安人, 博士, 中国科学院信息工程研究所助理研究员, 主要研究方向为网络安全、信息保护。