**个人权益保障技术体系与技术验证**

**总体技术方案**

|  |  |
| --- | --- |
| **课题名称：** | **个人权益保障技术体系与技术验证** |
| **课题编号：** | **2021YFB3101301** |
| **起止时间：** | **2021年12月-2024年11月** |
| **课题牵头单位：** | **中国科学院信息工程研究所** |
| **课题负责人：** | **李凤华** |
| **编制日期：** | **2022年5月** |
|  |  |

版本记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **作者** | **参与者** | **变更内容概要** | **编制/修订日期** |
| 0.1 | 李凤华 | 郭云川、牛犇、张玲翠、何媛媛、许晓耕 | 新建 | 2022年4月12日 |
| 1.0 | 李凤华 | 郭云川、牛犇、张玲翠、何媛媛、许晓耕、李子孚 | 根据内部评审意见修改 | 2022年5月16日 |
|  |  |  |  |  |

**目 录**

[一、文档介绍 1](#_Toc123252916)

[1.1 文档目的 1](#_Toc123252917)

[1.2 文档范围 1](#_Toc123252918)

[1.3 读者对象 1](#_Toc123252919)

[1.4 术语与解释 2](#_Toc123252920)

[1.5 依据文件 3](#_Toc123252921)

[1.6 文档概览 3](#_Toc123252922)

[二、需求背景及国内外发展状况 5](#_Toc123252923)

[2.1 课题概述 5](#_Toc123252924)

[2.2 课题需求分析 5](#_Toc123252925)

[2.2.1 个人权益保障技术架构需求分析 6](#_Toc123252926)

[2.2.2 全生命周期权益控制需求分析 7](#_Toc123252927)

[2.2.3 个人信息共享的延伸控制需求分析 7](#_Toc123252928)

[2.2.4 隐私信息确权机制需求分析 9](#_Toc123252929)

[2.2.5个人权益保障标准需求分析 10](#_Toc123252930)

[2.3 国内外发展现状与发展趋势 11](#_Toc123252931)

[2.3.1 个人权益保障技术架构 11](#_Toc123252932)

[2.3.2 全生命周期权益控制 16](#_Toc123252933)

[2.3.3 个人信息共享的延伸控制 19](#_Toc123252934)

[2.3.4 隐私信息确权机制 22](#_Toc123252935)

[2.3.5 个人信息保护标准体系 24](#_Toc123252936)

[三、课题目标及考核指标、测评方法等 34](#_Toc123252937)

[3.1 课题目标 34](#_Toc123252938)

[3.2 课题考核指标及测评方法 34](#_Toc123252939)

[3.3 课题成果的呈现形式及描述 35](#_Toc123252940)

[3.3.1 软件系统 35](#_Toc123252941)

[3.3.2 知识产权 35](#_Toc123252942)

[3.4 预期经济社会效益 35](#_Toc123252943)

[四、技术方案与技术路线 37](#_Toc123252944)

[4.1 总体设计思路 37](#_Toc123252945)

[4.1.1 课题间关系、课题研究内容间关系 37](#_Toc123252946)

[4.1.1.1 课题间关系 37](#_Toc123252947)

[4.1.1.2 课题研究任务关系 38](#_Toc123252948)

[4.1.2 课题主要研究内容 39](#_Toc123252949)

[4.1.3 课题技术路线 39](#_Toc123252950)

[4.2 个人权益保障技术架构 40](#_Toc123252951)

[4.2.1 研究内容 40](#_Toc123252952)

[4.2.2 技术方案 40](#_Toc123252953)

[4.2.2.1 总体设计 40](#_Toc123252954)

[4.2.2.2 个人权益保障模型 42](#_Toc123252955)

[4.2.2.3 个人敏感信息按需脱敏控制模型 44](#_Toc123252956)

[4.2.2.4 完备可信删除模型 46](#_Toc123252957)

[4.2.2.5 服务商自监管和执法监管的协同模型 50](#_Toc123252958)

[4.2.2.6 隐私侵权取证架构 56](#_Toc123252959)

[4.2.2.7 归一化描述 59](#_Toc123252960)

[4.2.2.8 权益保障组件优化动态部署 61](#_Toc123252961)

[4.3 全生命周期权益控制 62](#_Toc123252962)

[4.3.1 研究内容 62](#_Toc123252963)

[4.3.2 技术方案 62](#_Toc123252964)

[4.3.2.1 总体设计 62](#_Toc123252965)

[4.3.2.2 生命周期权益控制模型与描述 63](#_Toc123252966)

[4.3.2.3 异常事件推送机制 66](#_Toc123252967)

[4.3.2.4 权益控制操作原语与安全交换 68](#_Toc123252968)

[4.3.2.5 控制策略冲突判定与有效性评估 71](#_Toc123252969)

[4.4 个人信息共享的延伸控制 73](#_Toc123252970)

[4.4.1 研究内容 73](#_Toc123252971)

[4.4.2 技术方案 73](#_Toc123252972)

[4.4.2.1 总体设计 73](#_Toc123252973)

[4.4.2.2 延伸控制模型 74](#_Toc123252974)

[4.4.2.3 延伸控制策略归一化描述与传递机制 76](#_Toc123252975)

[4.4.2.4 授权控制链构建与副本跟踪 79](#_Toc123252976)

[4.4.2.5 控制策略安全绑定 81](#_Toc123252977)

[4.4.2.6 权限动态调整与执行可验证 82](#_Toc123252978)

[4.4.2.7 自审计与强制审计的协同机制 85](#_Toc123252979)

[4.5 隐私信息确权机制 87](#_Toc123252980)

[4.5.1 研究内容 87](#_Toc123252981)

[4.5.2 技术方案 87](#_Toc123252982)

[4.5.2.1 总体设计 87](#_Toc123252983)

[4.5.2.2 个人信息权属确定与传递机制 89](#_Toc123252984)

[4.5.2.3 海量隐私个人信息权属高效可信验证 93](#_Toc123252985)

[4.5.2.4 授权合规性可信判定 94](#_Toc123252986)

[4.5.2.5 确权审计可信存证与验证 95](#_Toc123252987)

[4.6 个人权益保障标准体系 97](#_Toc123252988)

[4.7 隐私数据流转状态管理与存证系统设计 99](#_Toc123252989)

[4.7.1 系统架构 99](#_Toc123252990)

[4.7.2 技术架构 101](#_Toc123252991)

[4.7.3 系统功能 102](#_Toc123252992)

[4.7.4 接口设计 103](#_Toc123252993)

[五、需要突破的关键技术及其突破途径和方法 105](#_Toc123252994)

[5.1 面向泛在共享的个人权益保障技术架构 105](#_Toc123252995)

[5.1.1 问题描述 105](#_Toc123252996)

[5.1.2 突破途径和方法 105](#_Toc123252997)

[5.2 泛在共享的延伸控制机制 108](#_Toc123252998)

[5.2.1 问题描述 108](#_Toc123252999)

[5.2.2 突破途径和方法 109](#_Toc123253000)

[5.3 面向隐私信息流转的权属判定 111](#_Toc123253001)

[5.3.1 问题描述 111](#_Toc123253002)

[5.3.2 突破途径和方法 112](#_Toc123253003)

[六、已有研究基础 114](#_Toc123253004)

[七、进度安排与组织保障 116](#_Toc123253005)

[7.1 进度安排 116](#_Toc123253006)

[7.2 组织保障 117](#_Toc123253007)

2.3 国内外发展现状与发展趋势

2.3.1 个人权益保障技术架构

在如今大数据时代，数据已经成为了重要的组成部分，而个人信息的权益保护和数据应用安全方面也成为了重要的课题，全生命周期权益控制保障个人信息权益成为了一个技术难点，尤其是针对应对隐私数据流转动态随机、多模海量、应用场景复杂、全生命周期覆盖、全流程保障的局势发展状况。个人权益保障技术架构，必须适应于法律法规和各种标准。因此本小节从法律法规、技术研究的角度来讨论国内外发展现状。

在法律法规方面，国际上尚无敏感个人信息处理安全要求的标准，在通用数据保护条例（GDPR）中把揭示种族或民族、政治观点、宗教或哲学信仰、或工会成员的个人数据，遗传数据、唯一标识某自然人的生物特征数据、关于健康或关于自然人的性生活或性倾向的数据列为特别类别个人数据。2020年颁布的《加州隐私权法》（CPRA）引入了“敏感个人信息”，并给出了敏感个人信息的类别。从法律角度，个人权益主要包括：知情权、决定权、更正权、删除权、查阅权和复制权。《中华人民共和国个人信息保护法》定义这些权益，具体如下。

（1）知情权：①基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出，法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定；②个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意；③基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

（2）决定权：有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

（3）更正权：个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

（4）删除权：有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：①处理目的已实现、无法实现或者为实现处理目的不再必要；②个人信息处理者停止提供产品或者服务，或者保存期限已届满；③个人撤回同意；④个人信息处理者违反法律、行政法规或者违反约定处理个人信息；⑤法律、行政法规规定的其他情形；⑥法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

（5）查阅和复制权：①个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供；②个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

国内外对个人权益保障研究主要从法律法规和技术方面展开，下面分别讨论。在**法律法规**方面，2015年，李汶龙基于对欧盟所提出的被遗忘权的反思与借鉴，对大数据时代隐私保护的机制尝试展开了研究，探讨了被遗忘权的中国化和其与新闻传播的冲突及可能的解决机制[1] 。2016年，贾聪聪在借鉴国外个人权益保护措施的基础上，尝试进行了我国互联网征信下个人权益保护制度的建构，一定程度上缓和了个人权益保障与信息流动之间的冲突[2] 。2017年，文晓分析了欧盟与美国在网络消费者隐私权保护这一问题上的不同处理方法，指出欧盟的统一立法规制模式更适合我国[3] 。2019年，袁泉针对个人权益因未曾细化而难以落实保障措施这一困难，综合考量信息法益形态与利益主体等因素，提出了基于信息生命周期理论的个人信息分类标准，从而能够进一步对个人信息进行分类保护[4] 。田娅汝针对我国缺乏个人权益保护相关上位法、互联网征信业务不规范、监管体系不健全等问题，提出了建立个人信息权等单独立法、在征信行业细化个人知情权和同意权、加强互联网征信监管等个人权益保障对策[5] 。

2021年，余圣琪在分析工商业时代背景下传统法律对于数据保护困境的基础上，比照欧盟、美国等主流国家对于数据权利的保护模式，探究了数据权利对传统权利的变塑和重建，以期实现数据权利保护与促进数据流动的双核保护目标[6] 。范江波基于数据权益的属性和与欧盟、美国及日本的数据权益保护的对比分析，提出了数据权益保护的三条基本原则——“一般信息与敏感信息区别保护”、“增强数据收集的‘告知-同意’透明度”、“合理范围内的被遗忘权”[7] 。苗慧基于隐私相关理论，通过对隐私政策的文本分析建立了相应的测评模型，以期为改善政策、规范管理、保护隐私权益提供决策依据[8] 。

**权益保障架构包含了隐私计算架构、监管架构和存证。目前尚无从宏观上对个人权益保障技术架构开展的研究工作，相关技术主要聚焦于隐私计算架构、监管架构、完备删除、组件优化动态部署、隐私侵权取证等方面。**

在**隐私计算架构**方面，2016年，信工所李凤华[9] 提出了面向隐私信息全生命周期保护的隐私计算理论与关键技术，涵盖了隐私计算框架、隐私计算形式化定义、隐私计算的重要特性、隐私保护效果评估、算法设计准则、隐私计算语言、隐私计算框架下的取证技术等内容，从隐私信息的感知、度量、脱敏、延伸控制、评估、销毁等环节给出全生命周期隐私保护解决方案，为泛在互联环境下隐私信息保护奠定了理论基础与计算架构。

在**监管架构**方面， Wilson III于2005年提出了由政府机关、科研机构、公司企业、社会团体构成的四方监管模型[10] 。Solum提出了网络空间自生秩序和自我监管模型[11] 。这些研究工作主要关注合规监管模型的构建，所采用的建模方法包括本体论、UML、BPMN等。Pandit H J等在文献[12] [13] [14] 中给出了GDPR合规检查中本体模型的构建模式，完成了对数据主体、数据采集、数据存储、数据使用及处理、数据分享、数据使用依据等核心要素的形式化定义，并在W3C推荐的本体库PROV-O和P-Plan基础上构建了描述GDPR合规检查中数据起源本体模型GDPRov和合规检查本体模型GConsent。Jake Tom等[15] 在研究GDPR中实体以及实体间约束关系的基础上，利用UML建模方法建立了GDPR中数据主体、数据控制者、数据处理者监管主体之间的行为关系模型。文献[16] 基于the Open Digital Rights Language（ODRL）构建了复杂系统中数据合规监管模型，实现了企业责任的自动化合规检查。文献[17] 基于复杂事件处理系统研究了物联网这一高度动态变化和弹性伸缩环境下数据合规监管方法。然而，现有监管方面的研究更多关注合规性，缺少监管机构和企业间的协同监管，尤其是对监管架构如何部署、如何与信息系统集成、国家监管机构与企业内部监管机构的责权划分等方面的研究。

在**完备删除**方面，2015年，罗玉川提出了一种基于AONT的云数据可信删除机制，该机制将AONT转换与加密技术相结合，将原始数据转换为强不可分的密文数据，然后将密文数据的一部分同加密密钥一起销毁，从而提高了可信删除的有效性[18] 。2020年，程昱婷提出了一种基于用户权限撤销的数据可信删除方案，通过定义一个策略图将文件删除转化为策略撤销，随后再借助密文更新实现策略撤销，数据主体可以通过验证最新密文与原始密文生成的Merkle根节点是否一致来验证数据删除是否可信[19] 。郝嘉禄针对数据删除过程中存在的粗粒度、非即时、依赖第三方的问题，提出了一种基于细粒度策略的、自主控制的外包数据可信删除方案，基于已知难题的形式化安全性证明保证了该方案的安全性和可靠性，同时仿真结果表明了该方案可以以较低的开销满足数据可信删除的需求[20] 。2020年，Tian和Shao等人提出了一种基于椭圆曲线标量乘法的云数据可信删除方案，该方案显著提高了可信删除各个阶段的效率，同时实现了细粒度的访问与删除[21] 。2021年，Xie和Fu等人提出了一种基于强不可分性的云数据可信删除方案，通过结合异或运算与分组密码将密文数据变得强不可分，销毁任何一段密文数据都将导致原始数据的不可恢复[22] 。2022年，Tian和Wang提出了一种基于动态滑动窗口的可信删除方案，该方案通过Merkle树实现数据删除证明；采用多级安全思想和滑动窗口技术实现了更细粒度的访问控制[23] 。2022年，Tian和Wang提出了一种安全有效的有序覆盖删除方案（SEAD-OO），采用基于密文策略属性的加密实现了细粒度的访问控制和数据共享，引入物理删除和逻辑删除确保密文的删除，引入区块链确保删除的有效性和可追溯性[24] 。

在**组件优化动态部署**方面，2017年，吉振领提出了一种面向SLA的微服务动态部署方案，该方案构建了微服务动态部署描述模型和相应权值的动态更新机制，使用Docker容器包装微服务及运行时环境并以此为基础提出了微服务池模型，以一定的冗余保证了微服务的可用性[25] 。2020年，李旦提出了一种基于Prophet-LSTM组合的资源需求预测模型和相应的迁移时机判断方法，并通过实验证明了该预测模型比已有模型具备更高的预测精度[26] 。2021年，高雅卓等人结合完全信息静态博弈与马尔可夫决策过程，提出了一种基于多阶段随即博弈的虚拟化蜜罐动态部署机制（HoneyVDep），并以资源约束下防御方的综合收益最大化为目标建立了相应的优化模型[27] 。邵晓等人提出了一种基于强化学习的网络欺骗防御动态部署方案，该方案使用DQN算法寻找网络欺骗防御动态部署的最优策略[28] 。2015年，Sun和Wang等人提出了一种基于层次分析法的服务质量评估机制和动态正态分布选择方法进行服务部署的动态策略，采用动态惯性粒子群优化算法（DI-PSO）实现任务调度[29] 。2019年，Andrey和Anar实现了一个动态部署系统（DDS），自动化并显著简化了使用给定拓扑的用户定义流程及其对任何资源管理系统（RMS）的依赖关系的部署[30] 。2021年，Zhang和Jiao等人设计了一种基于流的增量调度器（Pool），将任务调度问题描述为最小成本最大流（MCMF）问题后，采用增量MCMF算法，加快了计算最优流的过程，并采用了以任务迁移成本最小化为目标的启发式的调度算法[31] 。

在**隐私侵权取证**方面，在隐私信息跨信息系统传播的过程中，溯源信息需要在不同信息系统间广泛交换。现有的溯源取证方案[32] [33] 大多聚焦于单一信息系统内部，当隐私信息流转出信息系统边界后，便失去控制和溯源取证能力，并没有针对多应用系统、多边界的隐私信息广泛动态流转场景中溯源取证问题提出解决方案。另一方面，现有信息系统中隐私信息与保护策略大多分开存储，例如基于起源信息的方案[34] [35] [36] ，将信息的演化脉络存储在起源信息中，当隐私信息离开信息系统后，便失去了隐私信息保护策略标准，无法对隐私信息是否违背隐私信息所有者意愿进行判断。

尽管已经有一些相关规范指南标准可以参考，但当今发展现状仍面临一些问题。

（1）由于隐私场景多变且多样，关于对应权益保护无法灵活匹配多变场景下的海量数据，隐私数据和对应权益保护目前没有建立一个有效且全面覆盖全生命周期的联系。

（2）国际上尚无敏感个人信息处理安全要求的标准，国内关于敏感个人信息处理安全要求也有所缺乏，相对应的权益保障也缺乏相关标准规定，对于各个数据流转生命周期过程对应标准仍需补充完善。

（3）现有方案缺乏统一的溯源信息汇聚和分析能力，难以实现对不同信息系统边界的采集汇总和溯源取证。

2.3.2 全生命周期权益控制

个人权益控制是指采集法律、管理、技术等手段确保个人知情权、决定权、更正权、删除权、查阅权和复制权。个人权益控制在技术层面主要体现在脱敏、删除和监管等不同维度。目前产业界和学术界都对个人权益控制展开了研究。

全生命周期的权益控制主要关注脱敏控制、删除控制和监管控制等方面。隐私信息在全生命周期流转传播过程中，不仅需要管控信息，更要结合信息的应用场景、敏感程度、保护需求等多维度因素，综合确定该信息在传播过程中对脱敏、删除和监管的控制要求，进而通过设置信息的传播控制策略，建立有效的信息分享/传播秩序。以下从信息传播控制、传播路径发现、策略冲突检测和消解等方面予以分析。

在全生命周期权益控制方面，亚马逊公司提出保障数据安全级别的举措，其发布的Macie通过机器学习和模式匹配识别AWS中的敏感数据，但仅局限于局部的脱敏环节，并未考虑与删除、监管的联动，难以支撑泛在受控共享；在共享按需控制方面，谷歌公司的RAPPOR系统采用本地化差分保护机制收集用户数据并进行统计、分析、挖掘等操作；苹果公司的iOS 14.5系统和iPadOS 14.5系统采用差分隐私、随机标识符、位置模糊处理等技术对用户个人信息脱敏处理，但脱敏技术局限于单一场景，且信息动态传播与删除缺乏有效关联，多副本不能完备删除；在权益保障协同监管方面，IBM Security Guardium Solution在识别和分类企业内敏感数据的基础上，提供数据活动实时监控和用户行为分析，发现针对敏感数据的异常行为并进行合规监管，但监管技术滞后于应用，且缺乏线上实时监管的有效技术手段。

在**信息传播控制**方面，可以从宏观和微观两个角度来分析。从宏观角度，信息的传播控制的目标可以理解为最小化某类信息的传播范围传播，常用的方法有基于网络结构优化的传播阻断方法和基于信息竞争的对立信源群体选择方法[37] 。基于网络结构优化的传播阻断方法是直接阻断了信息传播的关键路径，具有更加稳定快速的控制效果。主要有通过阻断一定数量的边、基于边集删除、线性阈值模型下贪心策略设计具有近似比、移除边集或节点集最小化网络的谱半径。但是在真实应用中，阻断某些传播边或者节点会有侵犯人权的风险，可能会招致批评。对应的基于信息竞争的对立信源群体选择方法选择一组节点组成“好”信息源群体，该群体在网络上发布并传播用于澄清“坏”信息的“好”信息。主要有将独立级联模型推广为竞争独立级联模型来选择信源群体选择算法、将线性阈值模型推广为竞争线性阈值模型来信源群体选择算法等。但这种方法仍是将背景立足于已经传播产生负面影响而进行补救，而不是从信息从第一次分享开始进行管控。从微观角度，信息传播控制可以以时间为依据，分为预前控制、过程中控制和滞后控制三种[38] 。由于信息的传播具有时序性，技术以外的控制方法都是属于一种个体的主观行为或者一种事后的补救措施。早期的信息传播控制技术大多运用过滤机制和分级机制，对信息的传播进行管理。

在**传播路径发现**方面，在信息交换的过程中，确定信息传输的路径尤为重要，因而衍生了各类路径发现协议。早期的路径发现协议，大多是为了检验网络的链路状况或者确定一条延时短、带宽快的路线，此类协议基本不对路径上节点的真伪进行识别，因而很容易被攻击者伪造或篡改。站在隐私保护的角度，信息传输路径可以划分到轨迹隐私的范畴，因而找到一种可信的路径发现协议，可以避免由于传输路径泄漏而导致的隐私风险。RFC1393[39] 中对Traceroute协议进行了详细解释。Augustin等[40] 通过描述路由跟踪过程中经常出现的异常方式，将它们归纳为环形、圆形和正方形，并据此提出一种公开可用的路由跟踪工具—配对路由追踪，利用该工具，可以提取追踪过程中异常方式的共性，并对原因进行可能性分析。F. Valentini等[41] 提出了两种不基于集中式网络监控系统的路径发现方法，其中一种适用于IPv6的网络环境下，另外一种IPv4和IPv6的网络环境均适用。最初的动态源路由协议只包含DSR基本的路由发现和路由维护机制，由D. B. Johnson[42] 于1994年提出，并于1996年发表了对DSR大部分的设计细节和初步仿真结果[43] 。K. A. Sivakumar等[44] 基于密码学提出了一种多源广播加密方案，确保没有通过合法性验证的节点无法加入到路径中，同时设计了一种安全路由发现协议，实现了对RREQs先验矛盾检测机制进行量化评估。C. Chandra等[45] 对原有DSR协议进行了改进。Prizada等[46] 提出了一种新型实用的方案，用于建立和维持网络中的可信路由。IETF工作组于2009年在RFC5440[47] 中提出了路径计算单元协议PCEP。Polito等[48] 通过域间的QoS路径拓展PCE架构，使得不同运营商在多个域端获得在不同资源领域的AA权限。Choi J S[49] 提出了一种用户移动回传混合拓扑自动发现协议MPLS-TP，利用分布式邻居发现协议收集邻居信息和构造拓扑关系，实现集中管控。Yannizzi等[50] 结合当前域间上下文网络模型，解决了如何建立域间LSP问题。Sudarshan Vasudevan等[51] 提出了一种类似于ALOHA邻居发现算法，无需预知节点数量及其同步，并允许节点异步执行相邻节点发现任务。Hu Y C等[52] 提出了一种Ad Hoc网络中的新型安全路由协议Ariadne，可以防止攻击者或者被攻陷节点通过损害未被攻陷的节点，还可以防止多种类型的拒绝服务攻击，具有很高的效率。Kim等[53] 构造了一种安全路由发现协议SRDP，通过使用聚合消息认证码或多重签名机制，该协议允许源节点对路径上的各节点进行认证，保证了在DSR中的安全路径发现过程。为保证数据包在可信路径上流转，Helen Bakhsh等[54] 基于无PKI的优化加密方案ICING，描述并评估了一种信任感知的基于位置的动态多路径发现协议，旨在找到MANETs网络中一条通往目的节点的可靠度最高、开销最小的路径。Safa等[55] 提出了一种基于聚类的新型可信路由协议（CBTRP），通过将网络组织为不相交的群集，持续检测节点活动行为，选择可信的和具有资格的节点处理相关路由活动，并及时改变数据包路由路径，避免了中间恶意节点攻击，保证数据安全高效的传输。Avramopoulos I等[56] 考虑在有攻击者的环境下提出了一种路由技术，只要在源节点和目的节点之间存在有一条无故障的路径，就可以保证将数据包从源节点交付至目的节点，且通信带宽开销、处理需求和额外成本均较低，甚至可以通过阻塞恶意节点通信来抵抗攻击。

在**策略冲突检测和消解**方面，Lupu[57] 研究了Ponder语言中策略形式一致性问题，在进行策略冲突检测时，Lupu将策略分解为主体、客体和行为3个要素。当2条策略的某个要素的作用域相互覆盖时，就会引起符号冲突。姚键等[58] 研究了分布式系统中元素之间的关系，并统一抽象成有向无环图模型，提出了一种应用有向无环图模型来检测分布式系统中安全策略冲突的定量方法。李瑞轩等[59] 针对静态职责分离策略与可用策略并存时，由于互斥的需求可能引发策略非一致性冲突问题，提出了基于优先级的冲突消解方法。针对基于关系的访问控制策略冲突检测问题，Sarkis等[60] 提出了通过分析策略元素之间的关系来检测策略对之间是否存在冲突。直接冲突可以通过分析策略元素之间是否存在重叠，间接冲突通过分析两个策略元素之间是否存在隐式关系。Deng等[61] 提出了访问控制策略冲突检测与消解机制，该机制通过构建访问控制策略中的资源索引树，基于资源依赖关系、条件重叠关系和访问控效果，实现访问控制策略冲突检测与消解。在控制策略的有效性评估方面，随着访问控制策略复杂度增加，访问控制策略评估效率影响着数据跨域流转控制的效率。Liu等[62] 提出一个XACML访问控制策略评估方案XEngine，该方案首先将访问控制策略转化成数字策略进而转化成树形的数据结构，提高访问控制评估效率。Liu等[63] 提出了一个访问控制策略快速评估算法，并在XEngine系统中实现了该算法。同时将XEngine系统与SUN的访问控制评估点（Policy Decision Point，PDP）的策略评估性能进行分析对比。Ngo等[64] 提出使用数据间隔分区聚合和决策图组合的方法来提高XACML访问控制策略评估效率。Ngo等[65] 提出了XACML逻辑模型和决策图的方法，通过语义分析把策略中复杂的逻辑表达式转换为决策树来提高访问控制决策效率。

2.3.3 个人信息共享的延伸控制

延伸控制的内涵随时代变化而演化，从延伸控制目标上看，在早期延伸控制主要聚焦于信息脱敏控制[9] ，逐渐演化到删除控制和监管控制[66] 。面向个人信息共享的延伸控制是指泛在互联环境下个人信息共享过程中全生命周期各环节数据操作的迭代控制、控制策略的动态调整、控制策略的可控传递、控制策略执行的可信审计。

在**数据操作的迭代控制**方面，Wang L等[67] [68] 定义了数据胶囊范式，并提出了保障数据收集、管理和处理合规的隐私警戒模型PRIVGUARD [68] 。其中，数据胶囊由数据、用于描述该数据的元数据及限制该数据处理方式的策略构成其代替数据本身成为了模型中的最小管控单元，从而确保策略随数据流动，但这些工作未考虑策略动态调整，忽略了迭代控制。李凤华等在2008年提出了基于行为的访问控制（Action-Based Access Control, ABAC）模型，该模型考虑环境等因素，结合角色和时态，可解决移动计算的信息系统中的访问控制问题，可看做延伸控制的雏形。进一步，2016年李凤华等[69] 提出了面向网络空间的访问控制模型（CoAC），并将之应用于社交网络中图片转发过程中造成的隐私泄露问题，该模型采用资源传播链和网络传播链来记录个人信息在跨系统跨生态圈的流转过程，基于资源/网络传播链实现数据受控二次/多次转发。支撑个人信息延伸控制；并基于CoAC设计了面向图片的延伸控制实施机制[70] ，该机制并将隐私保护策略嵌入到图片中，对后续用户的操作权限进行延伸控制，实现社交网络中隐私图片的流转控制。虽然在CoAC中首次提出了延伸控制的思想，可以支撑交换后数据的延伸控制，但该机制的核心目标是主体对客体在不同流转过程中知悉范围的控制，没有对交换后数据的脱敏、删除、监管实施迭代控制，也没有强调策略随数据绑定与流转。为此，李凤华等在隐私计算理论[66] 中首次提出迭代控制，其核心思想是在脱敏、删除、使用等过程中对跨系统交换场景下个人信息实施多次的按需控制。

在**控制策略调整**方面，目前权限自动调整主要包括两类：基于风险的权限调整和基于时间的权限调整。在基于风险的权限调整中，首先依据用户场景，定义数据访问所面临的风险指标；而后计算权限调整前和调整后所带来的风险，当风险小于预定阈值时，可调整访问权限[71-74]。基于时间的权限调整方案中，首先设定用户仅在某个时间域内对数据的访问权限，在系统执行过程中，一旦在超出预定时间域，系统自动检测并撤销或调整已分配权限[75] [76] 。此外，Yan等[77] 将上下文感知的信任与声誉评估集成到加密系统，提出了基于信任的访问控制方案，支持访问权限随策略动态变化而调整。**综上，现有访问权限的调整主要基于风险和时间等要素，尚未做到权限随访问场景变化而自适应调整。**

在**延伸控制策略传递**方面，目前延伸控制策略传递主要聚焦于策略黏贴(Sticky Policy)，即如何通过安全绑定来实现安全传递，为此Pearson等[78] 和Spyra等[79] 使用加密机制将策略与数据相关联，并对策略进行属性编码和匿名化处理以防止被恶意利用，为全生命周期内数据访问控制提供支持。在延伸控制策略执行方面，目前主要工作采用传播链主要用来跟踪、记录数据生成过程，即记录谁在什么条件下对数据进行了什么操作，并基于传播链来执行空中。其中传播链通常呈现为由实体及实体之间的因果依赖关系构成的复杂有向图，可用开放起源模型（The Open Provenance Model，OPM）来描述[80] 。继OPM之后，W3C提出了一个新的数据起源描述模型PROV[81] 。Park等[82] 提出了基于起源的访问控制（Provenance-based Access Control，PBAC），利用起源数据实现访问控制。李凤华等[70] 在数据使用策略嵌入图片EXIF信息中来实现了图片的策略跟随，并利用公钥密码基础（PKI, public key infrastructure）保证策略的机密性和完整性。

在**控制策略执行审计**方面，Butin D等[83] 为策略跟随场景设计了基于日志的策略执行检查模型。在该模型中，日志由一组日志事件组成，一个日志事件用一个不定长的元组来表示，即不同类型的日志事件元组中包含不同的元素。考虑到日志是一个蕴含了时态信息的数据处理活动序列，Arfelt E等[84] 使用度量一阶时态逻辑（metric first-order temporal logic，MFOTL）对GDPR的部分相关条款进行了形式化，并使用MonPoly日志监控工具[85] 来检查执行的合规性。但这些工作未做到个人信息侵权行为泛在随遇实时判定与审计。

总体而言,国内外均对延伸控制了进行了研究，本课题组提出了延伸控制模型，但在个人信息保护中尤其是在大数据时代下个人信息保护中，数据延伸控制需求也越来越广泛，如何确保在个人数据交换出管理域后，数据拥有者仍能控制数据的使用行为，非常需要进一步探索。尤其是**如何对跨系统跨生态圈的数据操作执行迭代控制**、**如何准确构建并动态调整延伸控制策略、如何验证延伸控制策略被准确执行并确保可信审计**等方面需要进一步探索。

**（1）如何对跨系统跨生态圈的数据操作执行迭代控制**：当个人信息跨系统跨生态圈流转后，信息主体或数据提供方可能变更和动态调整控制意图；控制意图的动态变更需要及时反馈到跨系统跨生态圈的操作执行者。然后在跨系统跨生态圈时难以准确跟踪数据的流动（特别是对衍生数据），此外跨系统跨生态圈间的主体可能互不信任，即使相互信任，也可能没有统一的交互接口，因此如何实现跨系统跨生态圈的数据操作执行迭代控制是一大挑战。

**（2）如何准确构建并动态调整延伸控制策略**：延伸控制策略从“何时何地被谁以怎样的方式使用、使用后将被怎样处理”等角度定义交换后数据的使用方式。传统访问控制适合于单一组织形态的封闭环境，在这种封闭环境下不存在利益冲突，策略制定者可自行决定主体的访问权限。但在动态且难以预测的个人数据跨管理域流动中，数据提供者和提供者间存在利益冲突，策略不能仅由单方制定，数据提供者和使用者需要协商延伸控制策略。协商过程具有信息不完备性，如何在不完备信息下协商并动态调整延伸控制策略（包括利益攸关方的使用权限和义务）是另一个重要挑战。

**（3）如何验证延伸控制策略被准确执行并确保可信审计**：由于数据提供者和使用者在数据的使用方面通常存在利益冲突，因此数据所在管理域的主体不会完全信任其他管理域的主体，即使双方在策略协商阶段就个人数据的延伸控制策略达成了一致，提供者也可能担心对方是否准确执行协商后的该策略。在不可信环境下如何验证对方协商的策略准确执行也是一大难点，在对方不可信执行的情况下，如何进行可信审计也是挑战。

2.3.4 隐私信息确权机制

数据确权的主要目标分析数据所有权,重点是对数据资源整体链条上对数据使用和收益的权利分配。目前隐私信息确权研究主要聚焦于确权相关法律法规的制定。

早在上世纪80年代，数据资源的权属问题己经引起了国内外社会的关注｡就国外而言，多年来，涌现出了大量的关于数据确权方面的研究人员，澳大利亚学者Pendleton作为数据信息领域先驱,开创了国外信息产权问题。国外的相关研究更多地集中在数据的资源属性､产权分配制度以及数据所有权｡如Schwartz[86] 将个人信息或数据视为可以自由转让和流通的无形商品，并提出了由五项内容组成的法律保护模式，形成一个既尊重个人隐私又维护民主秩序的市场。由于数据可以被多方控制，相互间的控制不会影响其价值和使用，自然人数据权益的基本保护、开放与自由的流动保护是隐私信息保护的双重核心[87] 。从经济的角度，Dosis[88] 研究了产权对数据使用的影响，考虑隐私信息的服务价值和数据提取的隐私成本，在数据处理问题和过度货币化之间实现权衡。武西锋[89] 在学术界角度关于数据确权理论提出政府监管、个人所有、平台使用理应是我国数据确权的最优选择。

从技术角度，现有的隐私信息确权研究主要包括：基于数字版权的数据确权、基于区跨链的数据确权。**基于数字版权的数据确权**方面的研究工作包括：基于水印的权属追溯、基于区块链的数字版权保护方法。在基于水印的权属追溯方面，E.Mahmoud等人[90] 设计了一种基于时间戳的盲可逆关系数据库水印算法，确保数据在流转中可有效确认权属。Khanduja等人[91] 通过计算元组主键的ASCII码总和，来进一步确定要加入到属性中的符号，然后在选定元组的每一个候选属性值末尾加入相应字符从而实现水印嵌入。李文玲等[92] 设计并实现了一个对用户及其数据资源实现数据确权追溯等功能的关系型敏感数据防护系统。

在**基于区块链的数据确权**方面，吕俊[93] 等提出了一种区块链与社交网络传播链“双链融合”的安全传播机制，并在其基础上设计了一种数字版权服务区块链方案。郝海琳[94] 指出之前的数字签名作为不可见水印的方式较为复杂，采用了JUNA作为可见水印，实现了低空耗、低时耗和低成本的数字版权保护。余俊等人[95] 充分运用了区块链技术对数据确权的具体方法展开构建，找到“分布式架构”与“扁平化治理路径”的契合之处。Gao等[96] 提出了一种基于区块链和局部敏感哈希的数据确权机制，利用区块链技术解决数据确权的信任问题，再利用基于敏感哈希的数据指纹提取方案以保持指纹与数据的一致性。在云数据外包方面柳玉东等[97] 基于默克尔哈希树算法，设计并实现了一种全生命周期的云外包数据安全审计协议，保证了数据的隐私性与安全性。

总体而言，国内外均在较早使其就开始对数据确权进行了定义，逐渐在发展的过程中形成了数据确权的框架，但在实际生活中尤其是在大数据时代，数据交易所带来的数据确权问题变得更为尖锐，在**数据权属确定与审计机制、授权合规性快速判定等方面**需要进一步探索。

**（1）数据权属确定与审计机制**。个人信息在流动过程中存在两种情况：原始数据和衍生数据。由于原始数据可能隶属于多个拥有者，且多方参与了衍生数据生成，因此其权属分散性；由于数据的海量性、多模态性等特征，这使得不可能手工确定数据权属，因此研究海量多模态数据的自动确权机制是未来发展趋势之一，包括数据特征与数据摘要提取、数据目录等。此外，数据海量性、异构性、多模态性等使得需要自动化确权，然而由于数据权属确定受诸多方面影响（如法律因素、个人意愿、数据语义等），因此自动化确权可能存在错误；此外，数据权属传递处于不可控环境下，可能被非授权修改，因此数据权属确定与审计机制也是未来发展趋势之一，包括：交易确认、数据完整性度量、可信存证等。

**（2）授权合规性快速判定**。个人数据利用中存在诸多利益冲突的相关者、数据使用授权可能动态变化，这使得数据使用可能存在不合规状态；由于在特定场景下需要频繁合规性验证，而且业务逻辑的复杂性和合规性验证的复杂度高（通常属于NP完全问题），因此，如何快速判定授权的合规性是未来发展趋势。

2.3.5 个人信息保护标准体系

国际标准方面，国际标准化组织/国际电工委员会的第一联合技术委员会信息安全、网络安全和隐私保护分技术委员会第五工作组（简称ISO/IEC JTC1 SC27 WG5）专门负责网络安全领域的身份管理、生物识别安全和隐私保护方面的标准和指南的制修订工作。**隐私保护类标准**共27项，其中已发布15项，在研12项。ISO/IEC 27001:2013 信息安全管理体系是信息安全领域的重要标准，是建立信息安全管理体系的一套规范，标准详细说明了建立、实施及维护信息安全管理体系的要求，指出实施组织应该遵循风险评估标准。ISO/IEC 27002:2013 信息安全控制实用规则是ISO/IEC 27001提供风险处置具体的控制目标和控制措施指南，可以服务于开发组织的安全标准和有效的安全管理实践。ISO/IEC 27018:2019 公有云个人隐私保护提供了一套用于公有云中个人信息处理者的个人信息保护实用规则，以应对云服务中个人隐私保护的特定风险。ISO/IEC 27701:2019 隐私管理体系作为ISO/IEC 27001与ISO/IEC 27002在管理上的延伸标准，其目标是通过新增的要求来增强现有信息安全管理体系（ISMS）,以便建立、实施、维护和不断改进隐私信息管理体系（PIMS），标准概述了适用于个人身份信息（PII）控制者和PII处理者的框架，用于隐私控制管理，以降低个人隐私的各种风险。ISO/IEC 29134:2017 隐私影响评估指南提供了评估信息系统，程序，软件模块，设备或其他处理个人身份信息(PII)的活动对隐私的潜在影响的工具，以及隐私影响评估的主要步骤。ISO/IEC 29151:2017 个人隐私保护标准是通用的个人隐私保护标准，基于ISO/IEC 27002的各个域中加入了PII的事实指南，同时引入了ISO/IEC 29100十一大隐私保护原则，充分控制PII相关的风险和满足影响评估所确定的要求。**生物识别安全类标准**共4项，其中已发布2项，在研2项。ISO/IEC 24745:2022 生物特征信息保护为生物特征信息的安全和隐私兼容管理和处理提出了安全要求和建议，是生物特征信息处理过程中的个人信息保护指南。ISO/IEC DIS 27553-1和ISO/IEC NP 27553-2分别研究本地模式和远程模式下移动设备使用生物特征认证的安全和隐私要求。

国内标准方面，全国信息安全标准化技术委员会大数据安全标准特别工作组（简称TC260 SWG-BDS）负责个人信息保护相关国家标准的制修订工作。在基础共性类标准中，已发布个人信息保护基础安全标准2项规范标准和1项实施指南类标准。最基础的规范标准是GB/T 35273—2020 《个人信息安全规范》，规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动的原则和安全要求。GB/T 41391—2022《移动互联网应用程序（App）收集个人信息基本要求》规定了App收集个人信息的基本要求，给出了常见服务类型App必要个人信息范围和使用要求。GB/T 41574—2022 《公有云中个人信息保护实践指南》修改采用了ISO/IEC 27018:2019，给出了在公有云中实施个人信息保护的控制目标和控制措施，并给出了公有云个人信息保护指南。尚未发布面向个人信息权益保护安全框架、实现指南和个人敏感信息处理安全要求的通用基础共性类国家标准。

在技术标准中，仅发布了1项实施指南类标准。GB/T 37964—2019《个人信息去标识化指南》描述了个人信息去标识化的目的和原则，提出了去标识化过程和管理措施。尚未发布个人敏感信息分类分级、脱敏控制方法和算法选择方法、删除技术相关的国家标准。

在评估标准中，仅发布了1项标准。GB/T 39335—2020 《个人信息安全影响评估指南》给出了个人信息安全影响评估的基本原理和实施流程。尚未发布这妞个人信息处理效果评估与个人权益保障评估的国家标准。

综上，尽管在《个人信息保护法》指引下，我国的个人信息保护标准研制工作正在蓬勃开展，已经发布实施了多项通用的个人信息安全保护规范和指南，目前仍然存在如下问题。首先已有标准填补关键的个人信息保护标准空白，尚未形成体系化的个人信息保护标准框架，特别是在个人信息分类分级、脱敏控制、删除效果监测等方面需要制定相应标准。其次已有标准以提出安全原则、要求为主，亟需能够与之配套的实施细则或实施指南类标准，引导个人信息处理者切实通过有效的技术和管理手段满足安全要求。最后监管支撑标准和应用场景类国家标准目前仍然空缺。

**参考文献：**

1. 李汶龙. 大数据时代的隐私保护与被遗忘权[D].中国政法大学,2015.
2. 贾聪聪. 互联网征信法律问题研究[D].华东政法大学,2016.
3. 文晓. 网络交易中消费者隐私权法律保护模式研究[D].湘潭大学,2017.
4. 袁泉. 大数据背景下的个人信息分类保护制度研究[D].对外经济贸易大学,2019.
5. 田娅汝. 互联网征信中个人权益法律保护研究[D].河北科技大学,2019.DOI:10.27107/d.cnki.ghbku.2019.000385.
6. 余圣琪. 数据权利保护的模式与机制研究[D].华东政法大学,2021.DOI:10.27150/d.cnki.ghdzc.2021.000007.
7. 范江波.以个人数据权益保护为核心的大数据权益保护研究[J].信息安全研究,2021,7(12):1166-1177.
8. 苗慧. 中外移动APP的个人信息保护研究[D].北京邮电大学,2021.DOI:10.26969/d.cnki.gbydu.2021.002571.
9. 李凤华, 李晖, 贾焰, 等. 隐私计算研究范畴及发展趋势[J]. 通信学报, 2016, 37(04): 1-11.
10. Wilson E J. What is internet governance and where does it come from?[J]. Journal of Public Policy, 2005, 25(1): 29-50.
11. Solum L B . Models of Internet Governance[J]. Social Science Electronic Publishing, 2009:48-92.
12. Pandit H J, O'Sullivan D, Lewis D. An Ontology De-sign Pattern for Describing Personal Data in Privacy Policies[C]//WOP@ ISWC. 2018: 29-39.
13. Pandit H J, Lewis D. Modelling Provenance for GDPR Compliance using Linked Open Data Vocabu-laries[C]//PrivOn@ ISWC. 2017: 39-40.
14. Pandit H J, Debruyne C, O’Sullivan D, et al. GCon-sent-a consent ontology based on the GDPR[C]//European Semantic Web Conference. Springer, Cham, 2019: 270-282.
15. Tom J, Sing E, Matulevičius R. Conceptual representation of the GDPR: model and application directions[C]//International Confer-ence on Business Informatics Research. Springer, Cham, 2018: 18-28.
16. Tsohou A, Magkos M, Mouratidis H, et al. Privacy, security, legal and technology acceptance require-ments for a GDPR compliance plat-form[M]//Computer Security. Springer, Cham, 2019: 204-223.
17. Agarwal S, Steyskal S, Antunovic F, et al. Legislative compliance assessment: framework, model and GDPR instantiation[C]//Annual Privacy Forum. Springer, Cham, 2018: 131-149.
18. 罗玉川. 面向云存储的共享数据完整性审计和可信删除机制研究[D].国防科学技术大学,2015.
19. 程昱婷. 面向智慧医疗的属性隐私保护和数据可信删除研究[D].西安电子科技大学,2020.DOI:10.27389/d.cnki.gxadu.2020.003113.
20. 郝嘉禄. 云计算数据安全及访问控制关键技术研究[D].国防科技大学,2020.DOI:10.27052/d.cnki.gzjgu.2020.000039.
21. Tian Y, Shao T, Li Z. An efficient scheme of cloud data assured deletion[J]. Mobile Networks and Applications, 2021, 26(4): 1597-1608.
22. Xie Z, Fu W, Xu J, et al. Assured Deletion: A Scheme Based on Strong Nonseparability[J]. Journal of Sensors, 2022, 2022.
23. Tian J, Wang Z. Cloud data assured deletion scheme based on dynamic sliding window[J]. Peer-to-Peer Networking and Applications, 2022: 1-17.
24. Tian J, Zhang T. Secure and effective assured deletion scheme with orderly overwriting for cloud data[J]. The Journal of Supercomputing, 2022, 78(7): 9326-9354.
25. 吉振领. 云环境下微服务的动态部署研究[D].河南科技大学,2017.
26. 李旦. 面向动态资源需求的SaaS服务部署优化研究[D].西安电子科技大学,2020.DOI:10.27389/d.cnki.gxadu.2020.003117.
27. 高雅卓,刘亚群,张国敏, 等.基于多阶段博弈的虚拟化蜜罐动态部署机制[J].计算机科学,2021,48(10):294-300.
28. 邵晓,刘曼琳.基于强化学习的网络欺骗防御动态部署研究[J].网络安全技术与应用,2021(12):13-15.
29. Sun H, Wang S, Zhou F, et al. Dynamic Deployment and Scheduling Strategy for Dual-Service Pooling Based Hierarchical Cloud Service System in Intelligent Buildings[J]. IEEE Transactions on Cloud Computing, 2021.
30. Manafov A, Lebedev A. DDS Dynamic Deployment System[J]. GSI report, 2014, 2015.
31. Zhang M, Jiao P, Peng Y, et al. Efficient Dynamic Deployment of Simulation Tasks in Collaborative Cloud and Edge Environments[J]. Applied Sciences, 2022, 12(3): 1646.
32. 薛见新, 申德荣, 寇月, 等. 面向数据融合的半环溯源计算方法[J]. 计算机研究与发展, 2016, 53(02): 316-325.
33. 王梁, 周光焱, 王黎维, 等. 不确定关系数据属性级溯源表示与概率计算[J]. 软件学报, 2014, 25(4): 863-879.
34. Sun L, Park J, Nguyen D, et al. A provenance-aware access control framework with typed provenance[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(4): 411-423.
35. Park J, Nguyen D, SANDHU R. A provenance-based access control model[C]//The 10th Annual International Conference on Pri-vacy, Security and Trust.2012: 137-144.
36. Bates A M, Tian D, Butler K R B, et al. Trustworthy whole-system provenance for the Linux kernel[C]//The 24th USENIX security symposium. 2015: 319-334.
37. 吴鹏. 在线社交网络群体发现及其传播控制技术研究[D]. 上海: 上海交通大学
38. 巢乃鹏, 黄娴. 网络传播中的"谣言"现象研究[J]. 情报理论与实践, 2004, 27(6):5.
39. Malkin G. Traceroute using an IP option[S]. RFC 1393, IETF: Internet Engineering Task Force, 1993.
40. Birice Augustin, Xavier Cuvellier, Benjamin Orgogozo, et al. Avoiding traceroute anomalies with Pairs traceroute. In: Proceedings of the 6th ACM SIGCOM conference on Internet measurement (SIGCOM 2006), 2006:153-158.
41. F. Valentini, M. Pratesi, F. Santucci, et al. Ipv4 and ipv6 Troubleshooting Enhancement through Reverse Path Discover. In: Network Operations and Management Symposium (NOMS 2014), 2014:1-4.
42. Johnson D B. Routing in Ad Hoc Networks of Mobile Hosts. In：Mobile Computing Systems and Applications, 1994: 158-163.
43. Johnson D B, Maltz D A. Dynamic Source Routing in Ad Hoc Wireless networks[M]. Mobile computing, 1996, 153-181.
44. K.A. Sivakumar and M. Ramkumar. An Efficient Secure Route Discovery Protocol for DSR. In: In IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference, 2007: 458–463.
45. C. Chandra and V. Singh. Advance Dynamic Source Routing (ADSR) for Multi Hop Ad Hoc Network and Performance Evaluation of Proactive and Reactive Protocols. In: Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing, 2014: 1-24.
46. Asad Amir Prizada, Amitava Datta, Chris McDonald. Incoporating and Reputation in the DSR Protocol for Dependable Routing[J]. Computer Communications, 2006, 29(15): 2806-2821.
47. Vasseur J P, Le Roux J L. Path Computation Element (PCE) Communication Protocol (PCEP)[S]. RFC5440, IETF: The Internet Engineering Taskforce, 2009.
48. S. Greco Polito, M. Chamania, A. Jukan. Extending the Inter-Domain PCE Framework for Authentication and Authorization in GMPLS Networks. In: 2009 IEEE International Conference on Communications (ICC, 2009), 2009: 1-6.
49. J.S. Choi, A Hybrid Topology Discovery Protocol for Mobile Backhaul. In: Proceedings of the 16th Communications & Networking Symposium(CNS 2013), 2013: 1–4.
50. Marcelo Yannuzzi, Xavi Masip-Bruin, Sergio Sanchez, at el. On the Challenges of Establishing Disjoint QoS IP/MPLS Paths Across Multiple Domains[J]. IEEE Communications Magazine, 2007, 44(12): 60-66.
51. S. Vasudevan, M. Adler, D. Goeckel, et al. Efficient Algorithms for Neighbor Discovery in Wireless Networks[J], IEEE/ACM Trans. Netw., 2013, 21(1): 69-83.
52. Y. C. Hu, A. Perrig and D.B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks[J]. Wireless Networks, 2005, 11(1): 21–38.
53. J. Kim and G. Tsudik, Srdp: Secure Route Discovery for Dynamic Source Routing in Manets[J], Ad Hoc Networks, 2009, 7(6): 1097-1109.
54. H. Bakhsh, N. Zhang and A. Carpenter, Tadl: A Trust-Aware Dynamic Location-based Protocol Suite for Discovering Multiple Paths in Manets. In: Proceedings of the 2015 International Conference on Distributed Computing and Networking Proc(ACM ICDCN 2015), 2015: 1–10.
55. Haidar Safa, Hassan Artail, Diana Tabet. A Cluster-based Trust-Aware Routing Protocol for Mobile Ad Hoc Networks[J]. Wireless Networks, 2010, 16(4): 969-984.
56. Avramopoulos, H. Kobayashi, R. Wang, et al. Highly Secure and Efficient Routing. In: IEEE INFOCOM, 2004: 197–208.
57. Lupu E C, Sloman M. Conflicts in Policy-based Distributed Systems Management[J]. IEEE Transactions on Software Engineering, 1999, 25(6):852-869.
58. 姚键, 茅兵, 谢立. 一种基于有向图模型的安全策略冲突检测方法[J]. 计算机研究与发展, 2005, 42(7):1108-1114.
59. 李瑞轩, 鲁剑锋, 李添翼, 等. 一种访问控制策略非一致性冲突消解方法[J]. 计算机学报, 2013, 36(6):1210-1223.
60. Sarkis L C, Silva V T D, Braga C. Detecting Indirect Conflicts Between Access Control Policies. In: Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC 2016), 2016:1570-1572.
61. Deng F, Zhang L Y. Elimination of Policy Conflict To Improve the PDP Evaluation Performance[J].Journal of Network and Computer Applications, 2017, 80:45-57.
62. Liu A X, Chen F, Hwang J, et al. Xengine: A Fast and Scalable XACML Policy Evaluation Engine [J]. In ACM SIGMETRICS Performance Evaluation Review, 2008, 36(1):265-276.
63. Liu A X, Chen F, Hwang J, et al. Designing Fast and Scalable XACML Policy Evaluation Engines[J].IEEE Transactions on Computers, 2011,60(12):1802-1817.
64. Ngo C, Makkes M X, Demchenko Y, et al. Multi-Data-Types Interval Decision Diagrams for XACML Evaluation Engine. In: Proceedings of 11th Annual International Conference on The Privacy, Security and Trust (PST 2013), 2013:257-266.
65. Ngo C, Demchenko Y, Laat C D. Decision Diagrams for XACML Policy Evaluation and Management[J]. Computers & Security, 2015, 49:1-16.
66. 李凤华、李晖、牛犇. 隐私计算理论与技术. 人民邮电出版社. 2021.04
67. Wang L, Near J P, Somani N, et al. Data capsule: A new paradigm for automatic compliance with data privacy regulations[M]//Heterogeneous Data Management, Polystores, and Analytics for Healthcare. Springer, Cham, 2019: 3-23..
68. Wang L, Khan U, Near J, et al. PrivGuard: Privacy Regulation Compliance Made Easier[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 3753-3770.
69. 李凤华, 王彦超, 殷丽华, 等. 面向网络空间的访问控制模型[J]. 通信学报, 2016, 37(5): 9-20.
70. 李凤华, 孙哲, 牛犇, 等. 跨社交网络的隐私图片分享框架[J]. Journal on Communications, 2019.
71. Singh K, Bhola S, Lee W. xBook: Redesigning Privacy Control in Social Networking Platforms.[C]//USENIX Security Symposium. 2009: 249-266.
72. Khambhammettu H, Boulares S, ADI K, et al. A framework for Risk Assessment in Access Control Systems[J]. Computers & Security, 2013, 39: 86-103.
73. Miettinen M, Heuser S, Kronz W, et al. ConXsense: Automated Context Classification for Context-Aware Access Control[C]//Proceedings of the 9th ACM symposium on Information, Computer and Communications Security. 2014: 293-304.
74. Dos Santos D R, Westphall C M, Westphall C B. A dynamic Risk-based Access Control Architecture for Cloud Computing[C]//2014 IEEE Network Operations and Management Symposium (NOMS). 2014: 1-9.
75. 惠榛, 李昊, 张敏, 等. 面向医疗大数据的风险自适应的访问控制模型[J]. 通信学报, 2015, 12.
76. Ning J, Cao Z, Dong X, et al. Auditable $sigma$-time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(1): 94-105.
77. Yan Z, Li X, Wang M, et al. Flexible Data Access Control based on Trust and Reputation in Cloud Computing[J]. IEEE Transactions on Cloud Computing, 2015, 5(3): 485-498.
78. Pearson S, Casassa-mont M. Sticky Policies: An Approach for Managing Privacy Across Multiple Parties[J]. Computer, 2011, 44(9): 60-68.
79. Spyra G, Buchanan W J, Ekonomou E. Sticky Policies Approach within Cloud Computing[J]. Computers & Security, 2017, 70: 366-375.
80. Moreau L, Clifford B, Freire J, et al. The Open Provenance Model Core Specification (v1.1)[J]. Future Generation Computer Systems, 2011, 27(6): 743-756.
81. Missier P, Belhajjame K, Cheney J. The W3C PROV Family of Specifications for Modelling Provenance Metadata[C]//Proceedings of the 16th International Conference on Extending Database Technology. 2013: 773-776.
82. Park J, Nguyen D, Sandhu R. A Provenance-Based Access Control Model[C]//2012 Tenth Annual International Conference on Privacy, Security and Trust. 2012: 137-144.
83. Butin D, Métayer D L. Log analysis for data protection accountability[C]//International Symposium on Formal Methods. Springer, Cham, 2014: 163-178.
84. Arfelt E, Basin D, Debois S. Monitoring the GDPR[C]//European Symposium on Research in Computer Security. Springer, Cham, 2019: 681-699.
85. Basin D A, Klaedtke F, Zalinescu E. The MonPoly Monitoring Tool[J]. RV-CuBES, 2017, 3: 19-28.
86. Paul M. Schwartz. Property, Privacy, and Personal Data. Harvard Law Review, 2004, 117(7).
87. 李文. 网络个人数据的确权问题研究[D].吉林大学,2020.DOI:10.27162/d.cnki.gjlin.2020.000779.
88. A. Dosis and W. Sand-zantman, "The Ownership of Data," SSRN Electronic Journal, 01/01 2019, doi:10.2139/ssrn.3420680.
89. 武西锋,杜宴林. 经济正义视角下数据确权原则的建构性阐释[J].武汉大学学报(哲学社会科学版),2022,75(02):176-184.DOI:10.14086/j.cnki.wujss.2022.02.015.
90. Mahmoud E. Farfoura,Shi-Jinn Horng,Jui-Lin Lai,et al.A blind reversible method for watermarking relational databases based on a time-stamping protocol[J].  Expert Systems With Applications . 2012 (3)
91. Khanduja V,Khandelwal A,Madharaia A, et al. A robustwatermarking approach for non numeric relational database[C]//proceedingsof the International Conference on Communication,2012.
92. W. Li, J. Yan and Z. Zhang, "Relational Database Watermarking Based on Chinese Word Segmentation and Word Embedding," 2020 29th International Conference on Computer Communications and Networks (ICCCN), 2020, pp. 1-6, doi: 10.1109/ICCCN49398.2020.9209600.
93. 吕俊,张志勇,徐艳艳.基于区块链的社交网络数字版权保护方法[J].计算机工程与设计,2021,42(06):1562-1570.DOI:10.16208/j.issn1000-7024.2021.06.008.
94. H. Hao and S. Su, "Digital Copyright Protection Scheme Based on JUNA Lightweight Digital Signatures," 2012 Eighth International Conference on Computational Intelligence and Security, 2012, pp. 582-586, doi: 10.1109/CIS.2012.136.
95. 余俊,张潇.区块链技术与知识产权确权登记制度的现代化[J].知识产权,2020
96. Z. Gao, L. Cao and X. Du, "Data Right Confirmation Mechanism Based on Blockchain and Locality Sensitive Hashing," 2020 3rd International Conference on Hot Information-Centric Networking (HotICN), 2020, pp. 1-7, doi: 10.1109/HotICN50779.2020.9350779.
97. 柳玉东,王绪安,涂广升, 等.全生命周期的云外包数据安全审计协议[J].计算机应用,2019,39(07):1954-1958.