基于生命周期与风险防范双视角的数据流通安全技术体系

陈禹存[1]，黄科满[2]，杜小勇[2,3]
1. 中国人民大学统计学院，北京 100086；
2. 中国人民大学信息学院，北京 100086；
3. 数据工程与知识工程教育部重点实验室，北京 100086

摘要
随着大数据、云计算和人工智能的快速发展，数据流通安全治理面临新的挑战，亟须形成系统化、可持续增长的技术体系。从技术落地的角度出发，讨论了构建数据流通安全体系存在的问题，梳理了国外典型的数据安全技术体系。在此基础上，提出了数据流通安全治理技术体系框架，从数据流通生命周期和数据流通安全风险应对两个视角，构建了数据流通安全技术体系，包含在数据流通安全中发挥重要作用的49项技术。通过专家评审，从发展阶段、重要程度、技术潜力、落地难度等维度，剖析当前数据流通安全治理技术体系的发展情况和存在的问题。构建和完善数据流通安全技术体系，能够推动数据要素产业和数字经济健康持续发展。

关键词
数据流通安全；技术体系；数据流通；数据风险防范

中图分类号：TP309.2 文献标志码：A doi：10.11959/j.issn.2096-0271.2024064

A data circulation security technology system based on the dual perspectives of lifecycle and risk prevention

CHEN Yucun[1], HUANG Keman[2], DU Xiaoyong[2,3]
1. School of Statistics, Renmin University of China, Beijing 100086, China
2. School of Information, Renmin University of China, Beijing 100086, China
3. Key Laboratory of Data Engineering and Knowledge Engineering, Beijing 100086, China

Abstract
With the rapid development of big data, cloud computing, and artificial intelligence, data circulation security governance faces new challenges and requires a systematic and sustainable growth technology system. Starting from technology implementation perspective, this paper discusses the problems in building a data circulation security system and reviews typical data security technology frameworks from abroad. Based on this, this paper proposes a data circulation security governance technology framework. This framework organizes 49 key technologies that play important roles in data circulation security, constructed from two perspectives: data circulation lifecycle and responses to data circulation security risks. Based on expert evaluations, the development status and existing problem of the current technological frameworks for data circulation security governance are analyzed, from the dimensions of

development stage, importance, technological potential and implementation challenges. Building and improving a secure technology system for data circulation can promote the healthy and sustainable development of the data element industry and the digital economy.

Key words
data circulation security, technological system, data circulation, data risk prevention

0 引言

随着大数据、云计算、人工智能等的演进升级，数据的价值愈发凸显，经济社会发生系统性变革，驱动我国加速迈入数字化、网络化、智能化的数字时代。数据要素成为国家发展的重要助推器[1]。国家互联网信息办公室发布的《数字中国发展报告（2022年）》指出，2022年我国大数据产业规模达1.57万亿元，同比增长18%；《国家信息化发展报告（2023年）》指出，2023年我国大数据产业规模达1.74万亿元，同比增长10.45%。党的十九届四中全会提出，健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制。这是党中央首次将数据增列为新的生产要素。党的二十大报告多次提及数字领域关键词，提出“加快发展数字经济，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群”，对建设数字中国提出了更高的要求。而发展数字经济、加快培育发展数据要素市场，必须把保障数据安全放在突出位置。近年来，我国政府高度重视数据安全领域的工作，数据安全已经成为数据要素发展的基石。《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》明确提出：加强涉及国家利益、商业秘密、个人隐私的数据保护，加快推进数据安全、个人信息保护等领域基础性立法，强化数据资源全生命周期安全保护。

数据通过跨空间域、跨管辖域、跨信任域的流通过程，在不同场景中释放更大的价值[2]。数据流通发展态势迅猛，数据流通成为释放数据要素价值的关键方式[3]，但构建高效、安全的数据流通体系仍存在诸多阻碍。

首先，数据在流通中的风险是客观存在的，数据价值越大，风险越大。数据具有易复制、易篡改、多粒度、边际成本低、价值后验性、可替代性等特性，同一数据可被不同主体多次采集、存储，数据被一个主体使用时并不影响其他主体的使用。而数据携带了实体（如人、机构等）的隐私或者机密信息，数据价值越大，其在流通过程中的泄露风险就越大。

然后，数据在流通中的安全标准具有一定的主观性，难以统一。不同国家、地区和行业有不同的安全标准和要求，这些标准和要求可能存在显著差异，甚至冲突[4-5]。标准不统一可能导致流通成本增加等问题[6]。同时，不同主体对数据安全和隐私的判断具有主观性，在没有统一的隐私安全衡量标准下，数据流通风险具有一定的不确定性[7]。

最后，数据外循环的参与主体多，安全风险范围广，责任边界模糊。数据流通涉及数据的聚合、处理、发布、应用等多个阶段，每个环节的风险均不相同[8-9]。数据流通的参与主体多，包括数据提供方、数据接收方、第三方服务商以及监管机构等。不同参与主体的责任不同，其对数据

安全的监测能力差异较大，一旦发生数据泄露或其他安全事件，难以迅速确定责任方并采取有效的补救措施[10]。

针对以上问题，数据流通安全技术在促进数据的安全可信流通方面可发挥重要作用。数据流通安全技术体系的研究集中在两个方面：一是单一数据主体的数据流通安全风险，例如政务数据安全[11]、行业数据安全[12]、个人数据安全[13]；二是数据安全治理的具体技术，例如数据跨境流动[14]、数据要素市场[15]、基础设施建设[16]、数据要素流通[8]等。目前的研究缺乏对数据流通安全技术体系和具体数据流通安全技术的详细探讨，如数据流通安全技术的定义、边界与发展情况。综上所述，亟须构建一套面向数据流通的安全治理技术体系，聚焦于技术本身，为数据流通提供一套完善的安全技术指导。

本文首先从国外数据治理体系出发，分析与数据流通安全有关的技术，然后介绍基于生命周期与风险防范双视角的数据流通安全技术体系，最后结合专家评审意见，分析该技术体系的现状并进行展望。

1 国外数据安全技术体系

数据流通安全作为数据安全的重要组成部分，其技术体系中的技术应当源于数据安全技术体系。因此，本文从数据安全技术体系出发，研究国外数据安全技术体系中包含的数据安全技术，从中提取有关数据流通安全的技术。

1.1 2023年应用安全技术成熟度曲线

Gartner技术成熟度曲线是Gartner公司提出的分析工具，旨在描述新兴技术从初始概念到广泛应用的成熟过程。《2023年应用安全技术成熟度曲线》从业务效益、成熟度、市场渗透率等维度评价并分析当下备受关注的27种数据安全技术及服务的技术成熟度，将与数据安全有关的技术分为5个阶段，分别是技术萌芽期、期望膨胀期、泡沫破裂低谷期、稳步爬升恢复期、生产成熟期，具体如**图1**所示。

（1）技术萌芽期

技术刚被提出或实现，市场对其关注度高，少数对商业敏感、富有冒险精神的企业开始尝试。技术处在新兴阶段，尽管存在缺点，但其创新潜力引起了部分企业的兴趣。

（2）期望膨胀期

技术逐步成型，部分企业开始跟进，开发与该技术相关的应用。随着媒体的报道和初期成功案例的增多，技术的关注度逐步达到顶峰，但实际应用和效果往往不如预期。

（3）泡沫破裂低谷期

技术的局限和缺点逐步暴露，由于无法达到预期，市场兴趣和投资热度开始下降，媒体的关注度也显著下降。一些项目失败或被放弃，企业开始质疑技术的实际价值。

（4）稳步爬升恢复期

随着时间推移，技术细节逐渐成熟，优缺点越来越明显，企业开始理解其真正的应用价值。更多的供应商开发出实用的产品，成功进入实践阶段的案例增多，在市场上受到主要媒体与业界的关注。

（5）生产成熟期

经过不断的发展，技术变得稳定和成熟，被广泛应用于各种场景，市场占有率越来越高，进入稳定应用阶段，业界有了一致的评价。

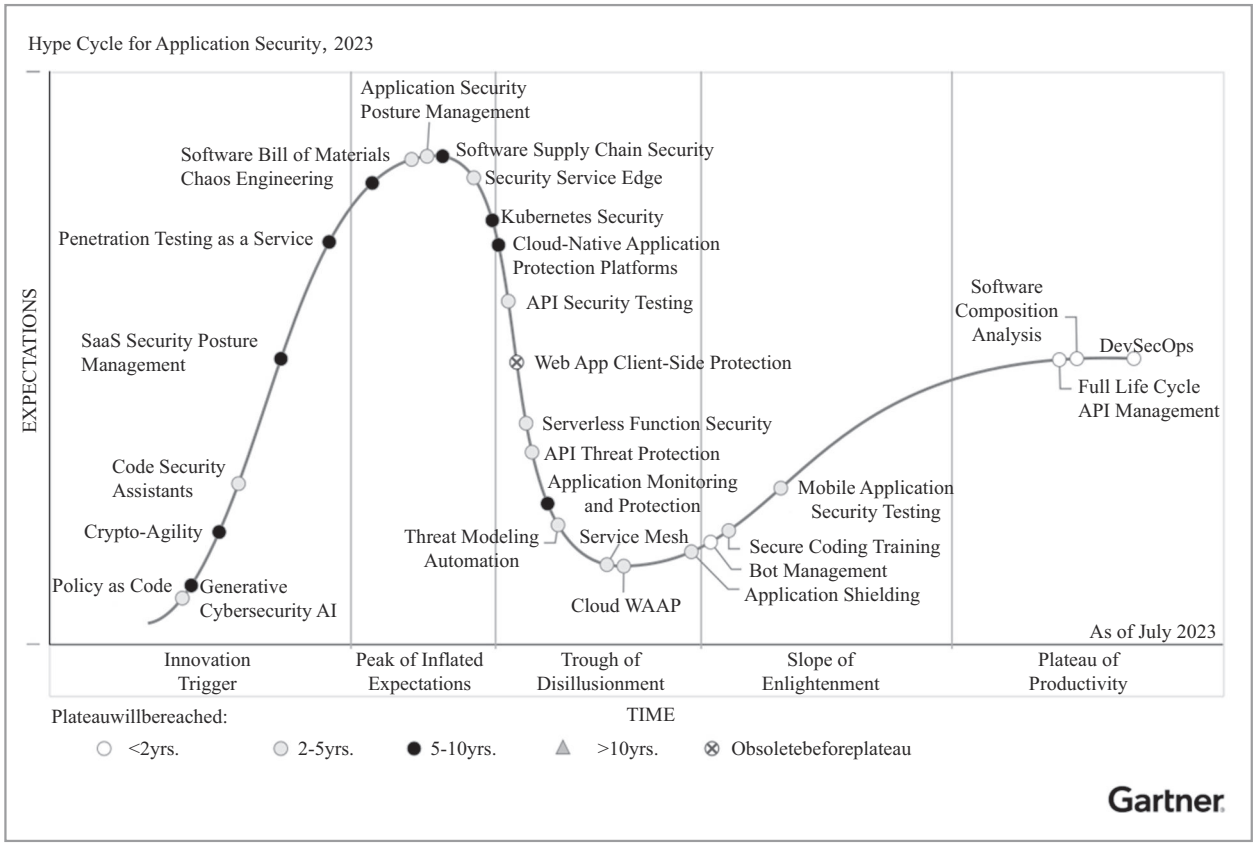

图1 Gartner数据安全技术体系[①]

1.2 IDC数据安全技术体系

IDC在2022年发布了《IDC TechScape：中国数据安全技术发展路线图，2022》，对中国数据安全市场进行系统化评估与分析，并对18个重要的数据安全技术进行了细致分析，给出IDC对于不同数据安全技术的定义和对其发展的理解，详细阐述了每个数据安全技术的发展程度、技术优势和劣势。此外，IDC对数据安全技术的市场采纳度进行了可视化展示。IDC数据安全技术体系根据技术的市场影响以及各技术的发展阶段，将技术分为变革型技术、主导型技术以及机会型技术，具体如图2所示。

（1）变革型技术

变革型技术将重塑市场及技术投资策略，可以创造新的市场机会和用户需求。此类技术通常与现有成熟技术存在较大区别，并且由于出现时间较短，其市场影响尚不明朗。

（2）主导型技术

主导型技术在当前数据安全领域中具有重要地位，处在不断迭代的发展期。

（3）机会型技术

此类技术多为在特定领域发挥作用的技术，其发展局限于具体的应用场景，而在改进数据安全的整体技术和流程方面的作用有限，如硬件安全模块。

2 数据流通安全治理技术体系

数据流通安全是数据安全的重要组成

[①] Gartner.《2023年应用安全技术成熟度曲线》. 2023.

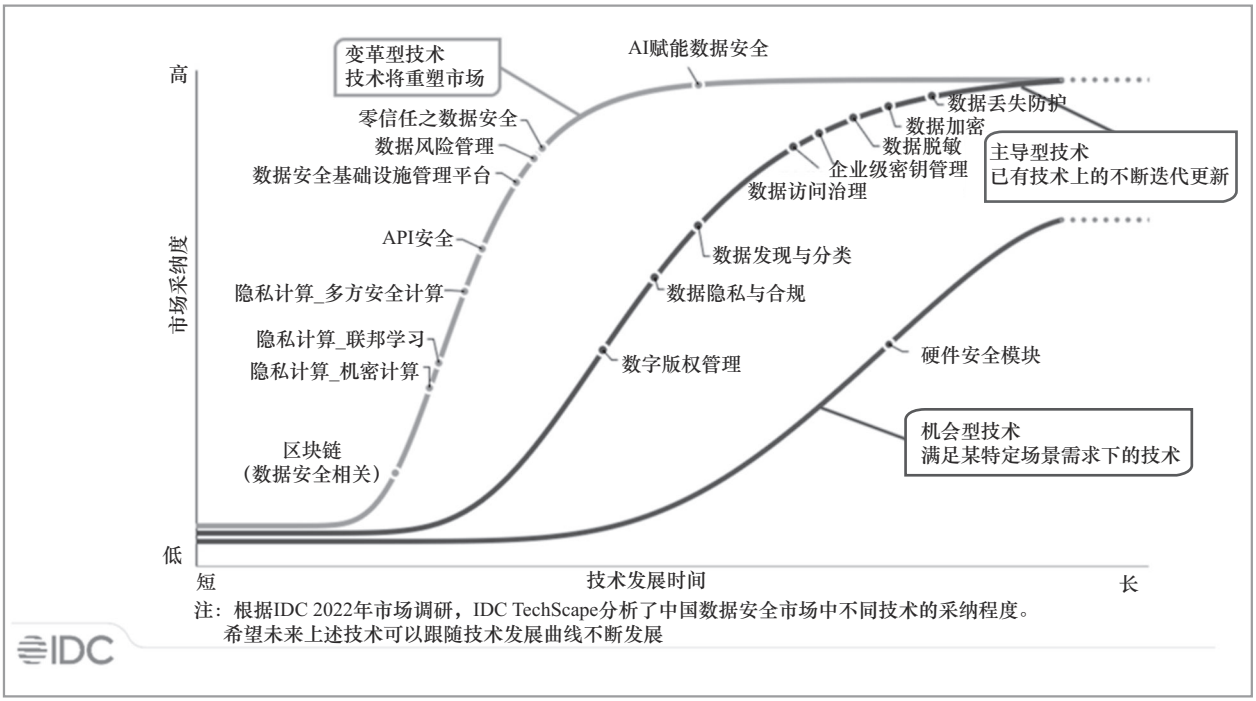

图2 IDC数据安全技术体系[②]

[②] IDC.《IDC TechScape：中国数据安全技术发展路线图，2022》. 2022.

部分。数据流通安全相关技术的发展仍处于起步阶段，目前数据流通仍然存在标准不统一、责任主体不明确、市场制度不健全等问题，而国内外数据安全技术体系各有侧重[17]，因此，构建一个全面、系统的数据流通安全技术体系尤为重要。本文围绕构建数据流通安全治理框架的目标，首先从数据流通生命周期出发，分析数据在不同流通阶段的具体情况，然后探讨数据在不同流通阶段中可能遇到的数据流通安全风险，最后基于数据要素流通价值生态模型，从数据流通生命周期与数据流通风险两个视角，梳理数据要素在流通的各个阶段所需的技术，从而构建数据流通安全技术体系。

表1 数据流通安全技术体系矩阵框架

阶段	数据组织汇聚	数据发布	数据流通应用
数据流通安全风险事前预防			
数据流通安全风险事中应对			
数据流通安全风险事后补救			

2.1 数据流通安全治理技术体系框架

基于数据流通生命周期和数据流通安全风险应对视角，构建如**表1**所示的技术体系矩阵框架。

表1的每一列代表数据流通的不同环节，每一行代表应对数据流通安全风险的不同阶段，矩阵中的元素代表了在某个数据流通环节中以及某个风险应对阶段中应具备的技术能力。例如，在数据组织汇聚活动中，事前预防阶段应具备的技术能力包括通过分级分类管控风险，事中应对阶段应具备的技术能力包括跟踪数据组织汇聚过程中可能导致分级分类变化的过程，

事后补救阶段应具备的技术能力包括当数据组织汇聚导致安全级别变化时，动态调整安全分类分级，并动态更新。

2.1.1 数据流通生命周期视角

从数据价值释放的角度出发，在跨域数据治理的框架中，数据管理需要经历3个关键阶段：数据组织汇聚、数据发布和数据流通应用。数据组织汇聚强调各个主体将组织内外部数据进行有效整合、汇聚到统一的数据底座中，并进行清洗、加工等一系列处理，通过数据标签化、对象化的组织方法，形成动态、可共享、可复用的数据资源，以供外部的应用和服务使用。数据发布强调将数据资源转化为可供其他应用程序、系统或用户使用的服务，对外发布，从而支撑数据资源的开放、共享和交易，以满足跨域业务协同的需求。数据可信流通更注重数据资源在不同主体之间的共享流通和开发利用，通过融合不同主体发布的数据服务，满足多方主体跨域业务的动态协同和跟踪审计。

（1）数据组织汇聚

在跨域数据治理的场景下，数据组织汇聚是数据资源全生命周期管理在跨域场景下的延伸，其主要目的是打破企业或组织中的数据孤岛状态，集成和整合组织内外部的数据资源，并通过搭建统一的数据底座，进行原始数据的清洗、加工、组织和加密等数据资源化生产过程。在此基础上，采用数据分级分类、数据加密等组织方法，对数据资源的全生命周期进行管理，以形成动态、可共享、可复用的数据资源。

数据组织汇聚是数据流通安全保障的基础环节。有效的组织和管理能够实现更高效的流通和共享，确保数据在全生命周期内安全、可控，为企业或组织的数字化转型发展和业务创新提供强有力的支持。

（2）数据发布

经过数据的组织汇聚，杂乱、无序、错误的原始数据被转化为有价值的、有组织的数据资源。数据资源应用到具体场景中，流通起来，才能更充分地释放数据的价值。然而，考虑到数据资源的质量、安全、隐私、权属等多方面因素，数据不能直接在各个主体之间进行共享、流通。数据发布是指将数据资源打包封装为可访问和可重复使用的数据服务或产品并对外提供的过程。在这个过程中，需要进行数据脱敏、密钥管理、访问控制等以保障数据发布过程的安全性与精准性，确保数据不会被泄露、被滥用等。

（3）数据流通应用

数据流通应用属于跨域数据治理的价值释放部分，旨在保障数据生产要素在不同主体之间被共享流通和开发利用，实现可信可靠的数据价值释放。在这个阶段，数据流通应用安全技术主要针对数据确权、数据安全应用监管、数据融合、数据溯源等方面的问题，保障数据在跨域流通环节中被安全应用，主要包括数据处理溯源、安全态势管理、数据访问控制等技术。

2.1.2 数据流通安全风险视角

在数据流通全生命周期中，安全风险是客观存在的。确定技术体系框架中数据流通不同阶段的应对措施，有助于降低数据流通中的安全风险[18]。数据流通中的风险应对包括3个阶段：事前预防、事中应对和事后补救。其中，事前预防强调在数据流通之前，识别并评估潜在的安全风险，并采取相应的防范措施；事中应对侧重于在数据流通过程中监控和应对安全事件，确保数据流通的安全和连续性；事后补救注重在安全事件发生后进行补救和恢复，减少损失并防止类似事件再次发生。

（1）事前预防

在跨域数据治理的场景下，事前预防是数据安全管理的第一道防线，其主要目的是在数据流通之前，识别和评估数据流通中潜在的安全风险，并采取相应的防范措施。这一阶段的重点是建立系统的风险管理机制，通过全面的风险评估和分析，确定风险的类型和等级，并制定相应的应对策略。

（2）事中应对

在数据流通过程中，事中应对是确保数据流通安全和连续性的关键环节。安全风险的事前预防无法完全保证数据流通过程中的安全，一旦遭受恶意攻击或者发生数据泄露、数据丢失等安全问题，事中应对技术能够及时发现和应对安全事件，防止影响范围继续扩大，确保数据流通的安全和连续性。

（3）事后补救

在安全事件发生后，事后补救是减少损失并防止类似事件再次发生的重要环节。这一阶段的重点是对安全事件进行详细分析和总结，明确事件发生的原因和影响范围，并进行数据恢复和修复，改进和优化现有的安全策略和措施。

2.2 数据流通安全技术体系

基于数据流通生命周期视角和数据流通安全风险应对视角，本文综合了上述的两个典型的国外数据安全技术体系以及国内代表性企业的数据流通安全治理体系，提取每个技术体系中有关数据流通安全的典型技术，形成了与数据流通安全治理相关的49项核心技术，并从技术落地的角度，对每项技术的定义、边界和应用场景做了界定。此外，根据每一项技术在数据流通安全领域的实际应用情况，将其划分为不同的发展阶段。数据流通安全技术体系见**表2**。其中，新兴技术代表这项技术处于诞生和研发阶

表2 数据流通安全技术体系

技术		具体内容	发展阶段与定位
AI赋能数据安全	生成式网络安全AI	是一种利用生成式人工智能模型（如生成对抗网络或大语言模型等），从源数据的大型存储库中学习，从而主动提高网络安全性的方法。其在合成和分析数据安全风险识别、生成数据风险防护建议、自动化风险应对等方面发挥重要作用	新兴技术
	代码安全助理	帮助开发人员识别和修复代码中的安全漏洞的技术。该技术有多种形式，如生成式人工智能、代码辅助器、自动语音提示等	
数据加密		通过成熟的算法、数据安全技术和特定层级的访问控制，为重要数据提供保护方案。加密技术已得到市场的广泛认可，其市场发展已进入成熟期	稳步发展
隐私计算	安全多方计算	计算参与多方能够在没有可信第三方的情况下，全程以密文形式联合多方信息，共同参与同一计算任务的隐私保护技术	快速发展
	可信计算	该技术从硬件层对使用中的数据进行加密、保护，能够在有多方参与的复杂协作环境中提供最高级别的安全隐私保护以满足合规要求	
	联邦学习	是一种分布式隐私保护建模方法，在所有训练数据不出域的前提下，多个参与方通过协作学习的方式共同训练新的数据模型	

续表

技术		具体内容	发展阶段与定位
数据脱敏		又称数据混淆，其运用多种不同的脱敏模板和脱敏算法修改数据内容，从而隐藏真实数据，保护敏感信息	技术成熟
数据分类分级		帮助组织主动进行信息与数据的生命周期管理，扫描与识别数据资产，并根据数据的敏感度进行分类分级，从而实施数据治理策略	快速发展
数据访问治理	身份鉴别	通过识别和验证不同数据实体的身份来确保数据的安全性和完整性，保护数据不被未经授权的个人或组织访问和修改以及防止数据在传输过程中被篡改或窃取	稳步发展
	访问控制	是在保障授权用户能获取所需资源的同时，拒绝非授权用户获取资源的安全机制，只有合法用户的合法访问才能被批准，而且只能在授权范围内进行访问	
数据处理溯源		数据源鉴别，对目标数据衍生前的原始数据来源进行监控，能预防数据泄露、恶意攻击等	快速发展
零信任网络访问		是一种新的访问安全与访问控制解决方案，专为“本地+远程”的复杂分布式网络环境设计	新兴技术
区块链（数据安全相关）		区块链为无中心、弱中心的场景提供数字信任证书，在数据交换的过程中，解决“数据确权”“难以篡改的数据使用留痕”“数据按约使用”等特定问题	新兴技术
数据安全基础设施管理平台		是从数据的发现与分类分级出发，集成数据合规治理、数据安全访问治理、敏感数据管理、数据防泄露、数据加密、数据脱敏等多种数据安全产品能力的统一安全监测、管理、运营平台。数据风险管理包括整体数据风险评估、风险监控与建模、风险缓解等，帮助用户清晰了解数据风险状况，并根据数据风险评估报告进行数据安全建设	新兴技术
数据安全态势管理		是一种网络安全技术，用于识别多个云环境和服务中的敏感数据，评估其对数据安全的威胁性和不合规风险	稳步发展
合成数据		是在原数据特征的基础上，通过算法、统计模型或生成式人工智能生成的数据，具有可控性强、数据量大、隐私保护能力强等优点	稳步发展
密钥管理与保密管理		对所有加密信息（包括公钥和公钥证书）的生成、分发、管理、计算和销毁进行集中管理的硬件和软件产品	稳步发展
数据丢失防护		是发现、监控和保护敏感数据的技术解决方案，可以发现、保护和控制静态、动态和使用中的敏感信息，旨在发现和阻断未授权使用和传输机密信息的行为	稳步发展
数据恢复		是确保数据在灾难发生后可以被恢复的技术和策略	稳步发展
安全信息与事件管理		用于实时分析安全警报和事件日志，帮助识别和应对潜在威胁	技术成熟
硬件安全模块		提供加密和强认证的密钥管理产品，可通过外部防篡改设备或计算机/服务器扩展槽的插入式串行卡进行交付。硬件安全模块配合企业密钥管理基础设施产品，在保护主加密证书等高价值数字资产的场景下落地实践	新兴技术
数据风险评估		是组织审查其控制下的敏感数据的过程，包括整个组织IT生态系统(包括所有平台、服务器位置和云环境)存储、访问和管理的所有数据	基础技术
API安全	API安全测试	是一种专门的应用程序安全测试(application security testing，AST)，旨在识别API中的漏洞，应检查传统应用程序漏洞(如注入攻击)和与API有关的安全问题(如中断对象级授权)	发展瓶颈
	API威胁保护	防止网页API被攻击和滥用以及访问违规。API网关、Web应用程序和API保护(Web application and API protection，WAAP)以及专门的API安全工具，通过对API参数和有效载荷的内容检查、流量管理和异常检测流量分析，为API提供保护	
	API全生命周期管理	从规划、设计到实施、测试、发布、运行、调用直至版本变更与退出的整个周期对API进行管理	技术成熟

续表

技术	具体内容	发展阶段与定位
灵活加密	是一种面对快速变化的安全需求和潜在威胁时，可以快速、透明地替换加密算法的方法，能够在不影响数据流通的情况下应对新出现的安全需求和漏洞	新兴技术
SaaS安全态势管理	SaaS安全态势管理(SaaS security posture management, SSPM)持续评估安全风险并管理SaaS应用程序的安全态势。SSPM工具提供了一系列功能，如识别本地SaaS安全设置并提供改进建议，管理身份权限，以及识别互连的SaaS应用程序。有些工具还能提供与行业框架、数据可见性和去中心化或完全自动化的补救措施的对比	新兴技术
PTaaS	渗透测试服务(penetration testing as a service, PTaaS)是一种基于技术驱动的服务。该技术在传统渗透测试的标准下，通过按需或持续性的应用程序和基础设施渗透测试发现安全隐患和提高安全性。它是一种创新的服务计算范式，在保护隐私的同时，优化设备端的智能模型训练过程。不同于传统的云计算、联邦学习与迁移学习范式，PTaaS通过SaaS平台提供，利用自动化和人工顶层(众包或供应商的内部团队)的混合方法来提高效率和有效性	新兴技术
混沌工程	利用实验性和潜在破坏性的故障测试或故障注入来发现分布式系统中的漏洞和弱点。混沌工程工具能够在系统的整个生命周期中系统地规划、记录、执行和分析对组件和整个系统的攻击。这种规划包括注入随机定时或攻击执行	快速发展
应用程序安全态势管理	应用安全态势管理(application security posture management, ASPM)是一类通过收集、分析和处理整个软件生命周期中的安全问题，持续管理应用风险的工具。ASPM通过对多个数据源的信息进行关联分析来执行安全策略，并按重要性排序，提供全面的风险视图	快速发展
软件材料清单	软件材料清单(software bil of materials, SBOM)是一种结构化的机器可读元数据，可唯一标识软件包。SBOM旨在跟踪和共享软件组件的详细信息及其跨组织的供应链关系，使整个软件供应链具有更高的透明度、更强的可审计性和可追溯性，加快安全和合规问题的解决	快速发展
软件供应链安全管理	是对软件开发生命周期各阶段实施的安全管理，确保从源代码到最终软件产品的整个过程都符合安全规范和标准。它涵盖了软件开发、供应商管理、交付、运营和维护等各个环节，旨在降低软件供应链中的安全风险	快速发展
安全服务边界	安全服务边界(security service edge, SSE)是通过保护对网络、云服务和私人应用程序的访问来确保安全的技术。SSE的功能包括自适应访问控制、数据安全、可见性和控制等。此外，它还具有高级威胁防御和合规使用控制机制。SSE提高了组织灵活性，确保Web和云服务以及远程工作的使用安全	快速发展
Kubernetes安全	Kubernetes安全是通过在Kubernetes容器编排平台上实施一系列安全流程、测试和控制措施来保障Kubernetes平台安全的技术。它与单独容器的安全性紧密结合，但侧重于Kubernetes的配置和准入控制	快速发展
云原生应用程序保护平台	云原生应用程序保护平台(cloud-native application protection platforms, CNAPP)在开发和生产过程中保护云原生应用。CNAPP整合了多个独立的功能，包括容器扫描、云安全态势管理、基础设施即代码(infrastructure as code, IaC)扫描、云基础设施授权管理和运行时工作负载保护	发展瓶颈
Web应用程序客户端保护	是一种安全创新，可抵御在客户端而非服务器端发起的应用程序级攻击。客户端保护可监控用户和应用程序的活动，并检测恶意操作和组件	发展瓶颈
无服务器功能安全	旨在处理无服务器功能保护的独特安全性和合规性要求。全面的解决方案从开发、授权和访问检查中的主动发现漏洞和配置扫描开始，通常与轻量级运行时保护和行为分析相结合	发展瓶颈

续表

技术	具体内容	发展阶段与定位
应用程序监控和保护	是结合应用程序的安全监控和操作监控以简化监控方式、减少监控工具的技术。这种结合可以在应用程序出现异常行为时，提醒应用所有者可能由于硬软件问题或者恶意攻击导致的服务故障。它还可以采取保护措施，如迁移工作负载、创建新实例、限制请求等	发展瓶颈
自动化威胁建模	自动化威胁建模工具可自动创建安全需求和威胁模型，可与软件开发生命周期工具集成，以管理需求并执行验证。自动化威胁建模工具能够动态地发现开发中功能需求带来的潜在安全隐患，并推荐安全编码实践或架构对策	发展瓶颈
云WAAP	云Web应用程序和API保护（WAAP）是一种缓解运行时攻击的技术，例如开放式Web应用程序安全项目的十大Web应用程序的安全漏洞，提供Web应用程序防火墙、分布式拒绝服务保护、机器人程序管理和API安全功能	发展瓶颈
数据价值评估	是对组织的数据资产进行评估、估值和定量分析的过程，旨在确定数据资产的价值、潜在利益以及相关的风险和机会。价值评估过程有助于识别和解决数据质量问题，提高数据的可靠性和价值	快速发展
服务网格	是一种分布式计算中间件，用于管理应用程序服务之间的通信，通常在托管的容器系统中被使用。它为服务间通信提供了轻量级中介，支持身份验证、授权、加密、服务发现、请求路由、负载平衡、自我修复和服务检测等。	发展瓶颈
应用程序防护	应用程序防护是一种应用程序内的保护技术，其功能直接在应用程序内实现，而不是在线或在主机系统上实现，可用于任何类型的应用程序，但目前特别关注移动应用程序	发展瓶颈
机器人管理	机器人管理解决方案可以检测和响应与网站、移动应用程序和API交互的自动化应用程序和机器人，可以阻止不需要的自动化活动，同时确保人类用户和合法机器人能够按照业务的意图进行访问。评估交互是否为人工操作，通常通过检查网络信号、设备和会话属性的分层方法来实现，通常通过向用户发送验证码的方式来解决问题	稳步发展
安全编码培训	提高了人们对源代码中漏洞的影响和预防措施的认识。开发人员参加特定编码语言和框架的安全编码实践培训，如实时培训、游戏化课程、视频、研讨会	稳步发展
移动应用程序安全测试	用于识别iOS和Android设备的移动应用程序中的漏洞。其通过分析代码、对程序进行攻击测试等方式识别应用程序在编码、设计、打包、部署和运行等环节中可能产生安全漏洞的条件	稳步发展
软件组成分析	软件组成分析产品是专门的应用程序安全工具，用于检测已知安全漏洞的开源软件和第三方组件，并识别潜在的不利许可和供应链风险。该技术能够确保软件供应链的安全与可信，提高应用程序开发的安全性	技术成熟
DevSecOps	DevSecOps将安全和合规测试集成到敏捷和开发运维管道中并实现自动化，尽可能无缝透明，不会降低开发人员的灵活性。理想情况下，DevSecOps还可以在运行时将安全性可视化	技术成熟
策略即代码	策略即代码（policy as code，PaC）语言将治理和合规规则表示为代码，可通过自动化工具以编程方式强制执行这些规则。PaC语言通常使用领域特定语言使政策能够像代码一样通过版本进行控制、审查和测试。成熟的PaC工具可以在代码中呈现大多数业务逻辑	新兴技术

段，具有较高的市场与外界关注度；快速发展代表这项技术已经初步具备实际应用的可能性，市场上有成功的案例可供参考；稳步发展代表这项技术的细节逐渐成熟，已经形成了一定规模的应用；技术成熟代表这项技术被各方广泛应用，有一定规模的市场；发展瓶颈代表这项技术因技术研发遇到困难或者市场需求降低而发展速度缓慢，处在瓶颈阶段。

为了从数据流通价值和风险应对两个维度理解这些关键技术，探讨当前数据流通安全技术体系的发展，我们邀请了28名领域专家，对这49项技术所处的数据流通阶段和数据流通安全风险应对阶段进行分类，其中24位专家完成了所有数据的填写。具体而言，针对每个技术，每位专家独立选择该技术所处的数据流通生命周期阶段以及其能够在数据流通安全风险的哪个应对阶段发挥作用。在此基础上，形成如**表3**所示的数据流通安全治理技术体系矩阵。

3 技术体系发展情况分析

为了探究数据流通安全技术的实际落地与应用情况，我们邀请每一位专家从重要性、落地困难程度以及技术潜力3个角度对每项技术进行打分。每一位专家评分时，需要在这49项技术中选择10项最重要、落地最困难、最有潜力的技术。数据流通安全治理技术体系中技术的得分见**表4**，每项技术的得分代表有多少位专家选择了该项技术，得分越高代表专家认为该项技术越重要，或者落地难度越大，或者潜力越大。

3.1 技术的受重视程度与其发展阶段的相关性强

由**表4**可知，技术的受重视程度与其发展阶段展现出了较强的相关性。除了数

表3 数据流通安全治理技术体系矩阵

阶段	数据组织汇聚	数据发布	数据流通应用
数据流通安全风险事前预防	生成式网络安全AI 数据加密 数据分类分级 区块链(数据安全相关) 数据安全态势管理 硬件安全模块 灵活加密 安全服务边界 数据价值评估 安全编码培训	生成式网络安全AI、安全多方计算、机密计算、数据脱敏、区块链(数据安全相关)、数据安全态势管理、合成数据、密钥管理与保密管理、数据丢失防护、安全信息与事件管理、数据风险评估、灵活加密、PTaaS、混沌工程、软件材料清单、安全服务边界、机器人管理、DevSecOps、零信任网络访问	生成式网络安全AI、代码安全助理、数据加密、联邦学习、身份鉴别、访问控制、API威胁保护、灵活加密、混沌工程、Kubernetes安全、云原生应用程序保护平台、无服务器功能安全、移动应用程序、安全测试软件组成分析、DevSecOps
数据流通安全风险事中应对	API安全测试	联邦学习、身份鉴别、访问控制、数据安全基础设施管理平台、API安全测试、API威胁保护、API全生命周期管理、SaaS安全态势管理、软件供应链安全管理、应用程序监控和保护、自动化威胁建模、云WAAP、服务网格、策略即代码	应用程序安全态势管理、云原生应用程序保护平台、Web应用程序客户端保护、无服务器功能安全、应用程序监控和保护、云WAAP、应用程序防护、API威胁保护
数据流通安全风险事后补救	—	数据处理溯源、数据恢复	数据处理溯源

表4 数据流通安全治理技术体系中技术的得分

技术名称	发展阶段	重要程度得分	技术潜力得分	落地难度得分
生成式网络安全AI	新兴技术	9	14	5
区块链(数据安全相关)	新兴技术	7	6	3
数据安全基础设施管理平台	新兴技术	6	5	2
策略即代码	新兴技术	2	4	1
零信任网络访问	新兴技术	2	2	5
PTaaS	新兴技术	2	2	3
灵活加密	新兴技术	2	1	7
SaaS安全态势管理	新兴技术	2	0	1
代码安全助理	新兴技术	1	5	1
移动应用程序安全测试	新兴技术	0	1	1
数据分类分级	快速发展	16	5	3
安全多方计算	快速发展	10	10	8
联邦学习	快速发展	9	11	4
机密计算	快速发展	9	3	6
数据处理溯源	快速发展	8	6	5
数据价值评估	快速发展	8	6	2
数据风险评估	快速发展	5	3	2
安全服务边界	快速发展	2	2	1
软件供应链安全管理	快速发展	1	2	2
应用程序安全态势管理	快速发展	1	0	2
混沌工程	快速发展	0	0	7
软件材料清单	快速发展	0	0	0
Kubernetes安全	快速发展	0	0	0
合成数据	稳步发展	9	12	7
身份鉴别	稳步发展	7	1	0
数据加密	稳步发展	6	2	2
访问控制	稳步发展	6	1	0
数据安全态势管理	稳步发展	4	3	5
数据恢复	稳步发展	4	0	3
安全编码培训	稳步发展	3	0	0
密钥管理与保密管理	稳步发展	2	0	0
硬件安全模块	稳步发展	1	3	2
数据丢失防护	稳步发展	1	1	2
机器人管理	稳步发展	0	3	1
数据脱敏	技术成熟	12	3	1
DevSecOps	技术成熟	2	3	3
API 全生命周期管理	技术成熟	2	1	0
安全信息与事件管理	技术成熟	1	0	0

续表

技术名称	发展阶段	重要程度得分	技术潜力得分	落地难度得分
软件组成分析	技术成熟	0	0	0
自动化威胁建模	发展瓶颈	2	0	0
云原生应用程序保护平台	发展瓶颈	1	1	1
API威胁保护	发展瓶颈	0	2	1
应用程序监控和保护	发展瓶颈	0	1	2
服务网格	发展瓶颈	0	1	1
云WAAP	发展瓶颈	0	1	0
API安全测试	发展瓶颈	0	1	0
无服务器功能安全	发展瓶颈	0	0	1
应用程序防护	发展瓶颈	0	0	0
Web应用程序客户端保护	发展瓶颈	0	0	0

据脱敏技术，大部分发展瓶颈阶段和成熟阶段的技术的重要程度得分和技术潜力得分非常低。而在最重要和最有潜力的技术中，新兴技术和快速发展的技术的比例最高，未来其将是数据流通安全技术治理体系的重要组成部分。同时，在重要程度得分和技术潜力排名前十的技术中，有8项技术相同，分别是：数据分类分级、安全多方计算、生成式网络安全AI、联邦学习、合成数据、数据处理溯源、数据价值评估、区块链（数据安全相关）。由此可见，技术的重要程度与其发展潜力密切相关。

生成式网络安全AI涵盖了数据流通价值活动的3个环节，数据分级分类和数据价值评估则着眼于数据组织汇聚阶段，合成数据为数据发布阶段提供了新思路。而数据安全基础设施管理平台、策略即代码等新兴技术，成为丰富数据流通安全风险应对策略的技术方向。

3.2 新兴技术和快速发展技术潜力巨大

数据流通安全技术中最有潜力的10项技术分别为生成式网络安全AI、合成数据、联邦学习、安全多方计算、数据处理溯源、区块链（数据安全相关）、数据价值评估、数据分类分级、数据安全基础设施管理平台、代码安全助理。这10项技术主要集中在数据发布与风险事前防范两个环节中。从数据流通生命周期视角来看，10项技术中有7项位于数据发布环节，3项位于数据组织汇聚环节，1项位于数据流通应用环节；从数据流通安全风险应对视角来看，10项技术中有8项位于事前预防环节，2项分别位于事中应对环节与事后补救环节。由此可见，除了数据发布阶段的技术，处于数据组织汇聚环节的技术逐渐被关注；风险应对策略正在往事中应对和事后补救环节发展。

从发展阶段来看，10项最有潜力的技术中，5项技术处于快速发展阶段，4项技术是新兴技术，合成数据是唯一处于稳步发展阶段的技术。由此可见，这些新兴技术以及处于快速发展的技术往往具有较大的技术潜力。

3.3 技术体系中技术分布不均衡

目前的技术体系中存在技术分布不均衡的问题，具体情况见**表5**和**表6**。从数据流通的视角来看，49项技术中，属于数据组织汇聚环节的技术仅有11项，而属于数据发布和数据流通应用环节的技术分别有35项和21项。从数据风险应对的视角来看，属于事后补救环节的技术仅有2项，而属于事前预防环节和事中应对的技术分别有39项和19项。数据组织汇聚环节和数据流通风险事后补救的技术较为缺乏。此外，在数据全生命周期流通中，数据销毁也是一个重要的过程，能否将数据销毁过程有关的技术纳入数据流通安全技术体系有待研究。

3.4 多项重要技术落地困难

多项在重要程度排名中靠前的技术，往往在落地难度方面的排名也靠前，如安全多方计算和机密计算，分别有10名和9名专家认为其很重要，其重要程度排名分别是第3和第6，落地难度排名分别是第1和第5。在数据流通安全技术体系建设中，许多先进技术已被提出，但在实际应用中仍面临以下困难。

（1）技术复杂性

许多先进的加密技术、数据访问控制机制和安全协议的理论被广泛研究，但由于技术复杂度高、部署难度大，在实际操作中难以部署和维护。

（2）成本高昂

高效的数据安全解决方案以及重要技术的发展，往往需要大量的硬件和软件投入以及专业人员的支持。成本高昂的问题在很大程度上限制了数据主体以及数据流通技术的发展。

（3）适配性不足

先进技术的实际应用场景不足，并且在不同应用场景中不同技术的适配性也不相同，难以满足各行业特定的数据流通安全需求。

4 结束语

本文在分析国外数据安全技术体系的基础上，从数据流通生命周期和数据流通风险应对两个角度出发，提出了覆盖数据流通各环节的数据流通安全技术体系框架，通过对数据流通安全领域中49项重要技术的评估，构建了双视角数据流通安全技术体系。目前，数据流通安全技术体系中的技术在实际落地中仍面临诸多挑战，迫切需要在强化数据组织汇聚阶段以及风险事后补救策略两个维度发力。未来的研究和实践应重点关注技术创新与应用落地，注

表5 数据流通生命周期视角下技术分布情况

技术所属环节	数据组织汇聚	数据发布	数据流通应用	数据组织汇聚+数据发布	数据组织汇聚+数据流通应用	数据发布+数据流通应用	全链条
技术数量	4	20	9	4	1	9	2

表6 数据安全风险应对视角下技术分布情况

技术所属环节	事前预防	事中应对	事后补救	事前预防+事中应对
技术数量	28	8	2	11

重全链条技术体系构建，增强数据流通安全技术体系的完整性。

数据流通安全技术体系是数据流通的重要保障，也是数据流通安全治理框架不可或缺的一环。构建和完善数据流通安全技术体系，为激活数据要素潜能和释放数据要素价值提供保障，推动数据要素产业和数字经济的健康可持续发展。

参考文献：

[1] 于施洋，王建冬，郭巧敏. 我国构建数据新型要素市场体系面临的挑战与对策[J]. 电子政务，2020(3): 2-12.
YU S Y, WANG J D, GUO Q M. Challenges and countermeasures of building a new data factor market system in China[J]. E-Government, 2020(3): 2-12.

[2] 柴云鹏，李彤，范举，等. 跨域数据管理的内涵与挑战[J]. 中国计算机学会通讯，2022，18(11): 37-40.
CHAI Y P, LI T, FAN J, et al.The connotation and challenges of cross-domain data management[J]. Communications of the China Computer Federation, 2022, 18(11): 37-40.

[3] 严宇，孟天广. 数据要素的类型学、产权归属及其治理逻辑[J]. 西安交通大学学报(社会科学版)，2022，42(2): 103-111.
YAN Y, MENG T G. Data typology, ownership and the governing principles[J]. Journal of Xi'an Jiaotong University (Social Sciences), 2022, 42(2): 103-111.

[4] 高志豪，郑荣，张默涵，等. 基于数据信托的产业数据要素流通：动力逻辑、信托纾困与模式重塑[J]. 情报理论与实践，2024，47(4): 75-83.
GAO Z H, ZHENG R, ZHANG M H, et al. Industrial data element circulation based on data trusts: power logic, trust relief and model remodeling[J]. Information Studies: Theory & Application, 2024, 47(4): 75-83.

[5] GAL M S, RUBINFELD D L. Data standardization[J]. New York University Law Review, 2019(4): 737-770.

[6] 高松. 数据跨境流通合规治理与技术实践[J]. 中国信息安全，2023(10): 75-79.
GAO S. Compliance governance and technical practice of data cross-border circulation[J]. China Information Security, 2023(10): 75-79.

[7] 王小乾. 数据要素合规流通的风险评估与防范[J]. 信息通信技术与政策，2024(4): 41-46.
WANG X Q. Risk assessment and prevention in the compliant circulation of data factors[J]. Information and Communications Technology and Policy, 2024(4): 41-46.

[8] 李凤华，李晖，牛犇，等. 数据要素流通与安全的研究范畴与未来发展趋势[J]. 通信学报，2024，45(5): 1-11.
LI F H, LI H, NIU B, et al. Research category and future development trend of data elements circulation and security[J]. Journal on Communications, 2024, 45(5): 1-11.

[9] 王文娟. 数据流通风险的识别与全流程治理路径[J]. 南昌大学学报(人文社会科学版)，2024，55(3): 88-98.
WANG W J. Identification of data circulation risks and full process governance paths[J]. Journal of Nanchang University (Humanities and Social Sciences), 2024, 55(3): 88-98.

[10] 高亚楠. 数据交易流通安全保障探索与研究[J]. 信息安全研究，2023，9(7): 662-666.
GAO Y N. Exploration and research on security guarantee of data transaction and circulation[J]. Journal of Information Security Research, 2023, 9(7): 662-666.

[11] 马广惠，安小米，宋懿. 业务驱动的政府大数据平台数据治理[J]. 情报资料工作，2018，39(1): 21-27.
MA G H, AN X M, SONG Y. Business-driven government big data platform data governance[J]. Information and Documentation Services, 2018, 39(1): 21-27.

[12] 林宏峥, 金维国, 宋国英, 等. 基于金融场景数据流通的安全技术研究[J]. 网络安全技术与应用, 2024(3): 105-107.
LIN H Z, JIN W G, SONG G Y, et al. Research on security technology of data circulation based on financial scenario[J]. Network Security Technology & Application, 2024(3): 105-107.

[13] 张媛媛. 论数字社会的个人隐私数据保护: 基于技术向善的价值导向[J]. 中国特色社会主义研究, 2022, 13(1): 52-59.
ZHANG Y Y. On personal privacy protection in digital society: taking technology for good as value orientation for example[J]. Studies on Socialism with Chinese Characteristics, 2022, 13(1): 52-59.

[14] 许可. 自由与安全: 数据跨境流动的中国方案[J]. 环球法律评论, 2021, 43(1): 22-37.
XU K. Freedom and security: the China plan for cross-border data flow[J]. Global Law Review, 2021, 43(1): 22-37.

[15] 马乐存, 裴雷, 李白杨. 数据要素流通安全治理: 体系架构与实践进路[J]. 农业图书情报学报, 2024, 36(3): 46-58.
MA L C, PEI L, LI B Y. Security governance of data element circulation: system architecture and practical approach[J]. Journal of Library and Information Science in Agriculture, 2024, 36(3): 46-58.

[16] 欧阳日辉. 数据基础设施保障数据安全及高效流通[J]. 人民论坛, 2024(7): 70-75.
OUYANG R H. Data infrastructure ensures data security and efficient circulation[J]. People's Tribune, 2024(7): 70-75.

[17] 鲍坤. 以要素流通为导向的数据权利理论及规范架构[J]. 上海大学学报(社会科学版), 2024, 41(4): 34-54.
BAO K. A data rights theory and regulatory framework oriented towards data element circulation[J]. Journal of Shanghai University (Social Sciences Edition), 2024, 41(4): 34-54.

[18] 刘业政, 宗兰芳, 金斗, 等. 数据要素流通使用的安全风险分析及应对策略[J]. 大数据, 2023, 9(2): 79-98.
LIU Y Z, ZONG L F, JIN D, et al. Security risk analysis and countermeasures in the circulation and use of data factors[J]. Big Data Research, 2023, 9(2): 79-98.

作者简介

陈禹存（2001– ），男，中国人民大学统计学院硕士生，主要研究方向为多模态、自然语言处理。

黄科满（1987– ），男，博士，中国人民大学信息学院副教授，中国人民大学吴玉章青年学者，麻省理工斯隆管理学院网络安全研究中心兼职研究员，国际网络安全专家CISSP认证。主要研究方向为数字生态、数据治理、网络安全治理。

杜小勇（1963– ），男，博士，中国人民大学吴玉章讲席教授、明理学院院长，数据工程与知识工程教育部重点实验室主任，中国计算机学会会士，国家数据标准委员会首批委员，国家信息技术标准委员会委员。主要研究方向为数据库与大数据技术、数据治理。

收稿日期: 2024-08-15

通信作者: 黄科满，keman@ruc.edu.cn

基金项目: 国家自然科学基金项目(No.62172425)；国家数据局课题 (No.SJ-ZC-2024004)；中国人民大学中央高校基本科研业务费专项资金项目(No.22XNKJ04)；中国科学院学部咨询评议项目(No.2023-ZW-02-A-013)

Foundation Items: National Natural Science Foundation of China(No. 62172425), National Data Bureau Project (No. SJ-ZC-2024004), Special Fund Project of Fundamental Research Funds for Central Universities of Renmin University of China(No. 22XNKJ04), Consultation and Evaluation Project of the Academic Divisions of Chinese Academy of Sciences(No.2023-ZW-02-A-013)