面向数据跨域安全流通的访问控制研究综述

李恒[1,2,3,4]，李凤华[1,2,3]，史欣怡[1,2,3]，郭云川[1,2,3]，郭守坤[1,2,3]
（1.中国科学院信息工程研究所，北京 100085；2.中国科学院大学网络空间安全学院，北京 100049；
3.网络空间安全防御全国重点实验室，北京 100085；4.自然资源部国家基础地理信息中心，北京 100830）

摘　要：为了解决数据要素流通中授权机制差异导致信息在系统中留存产生被篡改、被泄露和被滥用等安全风险，聚焦数据跨域安全流通主题，首先，从数据跨域访问控制面临的问题入手，对数据跨域流通基本概念和数据跨域访问控制内涵进行了深入研究。其次，针对数据跨域安全流通中的访问控制技术进行了全面综述，包括基于起源、基于意图和面向网络空间等访问控制模型；策略的标签挖掘、策略的协商与生成、策略的冲突检测与消解、策略的传递与执行、策略异常执行的审计等策略管理关键技术；基于区块链、基于数据胶囊和基于数据基础设施等策略实施机制。最后，对数据跨域流通面临的挑战及未来研究方向进行了总结与展望。

关键词：跨域访问控制；数据要素流通；数据使用控制；延伸控制；数据安全
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025042

Research on access control for secure cross-domain data circulation

LI Heng[1,2,3,4], LI Fenghua[1,2,3], SHI Xinyi[1,2,3], GUO Yunchuan[1,2,3], GUO Shoukun[1,2,3]
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. State Key Laboratory of Cyberspace Security Defense, Beijing 100085, China
4. National Geomatics Center of China, Ministry of Natural Resources of the People's Republic of China, Beijing 100830, China

Abstract: To address security risks such as tampering, leakage, and misuse of information stemming from inconsistent authorization mechanisms in data element circulation, the focus was placed on secure cross-domain data circulation. Initially, the challenges associated with cross-domain data access control were systematically examined, followed by an in-depth investigation into the fundamental concepts of cross-domain data circulation and the essential implications of cross-domain access control. Subsequently, a comprehensive review was conducted on access control technologies for secure cross-domain data circulation, which encompassed: access control models categorized as provenance-based, purpose-based, and cyberspace-oriented approaches; key policy management technologies involving label mining for policies, policy negotiation and generation, conflict detection and resolution, policy propagation and enforcement, and auditing of anomalous policy execution; policy implementation mechanisms developed based on blockchain technology, data capsules, and data infrastructure. Finally, current challenges in cross-domain data circulation are systematically summarized, and future research directions are proposed.

Keywords: cross-domain access control, data elements circulation, data usage control, extended control, data security

收稿日期：2024–10–10；**修回日期：**2025–02–28
通信作者：郭云川，guoyunchuan@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2023YFB3106304）；国家自然科学基金资助项目（No.U24A20240, No.62441226）
Foundation Items: The National Key Research and Development Program of China (No.2023YFB3106304), The National Natural Science Foundation of China (No.U24A20240, No.62441226)

0　引言

数据是数字经济的重要生产要素，是数字化转型的重要动力，已快速融入生产、分配、流通、消费和社会服务管理等各环节，深刻改变着生产生活方式和社会治理方式。不同组织或机构之间需要开放、交换、共享、使用和加工数据，以便更好地服务客户、提高效率和创造价值。数据需要在多个节点间传输，在流通的过程中可能会遭到未经授权的访问、篡改和滥用，因此，管控数据的跨域使用策略已成为数据要素流通的基本要求，面向数据跨域安全流通的访问控制技术也逐渐成为工业界和学术界新的关注焦点。

数据跨域安全流通是数据要素安全有序流转使用、充分释放数据价值的前提保障。访问控制技术是确保数据安全传输的重要手段，是保证数据安全有序流转的核心策略，也是数据安全治理的关键技术之一。访问控制技术[1]起源于 20 世纪 70 年代，由 Lampson 率先提出访问控制与机制的形式化描述，同时引入了主体、客体和访问矩阵概念，旨在确保资源只能经由授权实体以授权方式进行访问。早期的访问控制模型主要包括自主访问控制（DAC, discretionary access control）、强制访问控制（MAC, mandatory access control）和基于角色的访问控制（RBAC, role based access control）等基本类型[2-3]。随着操作系统、数据库、互联网等技术的发展，访问控制模型在早期模型基础上逐渐多样化。例如，基于 DAC 模型有面向数据库管理系统的 HRU（Harrison, Ruzzo& Ullman）模型、取予模型、框架保护模型（SPM, schematic protection model）和类型化访问矩阵（TAM, typed access matrix）模型等[4]；基于 MAC 模型有通过“下读，上写”多级安全机制的 BLP（Bell-LaPadula）模型、Biba 模型、中国墙（Chinese-wall）模型及域类型增强（DTE, domain and type enforcement）模型等[5-7]；RBAC 模型有扩展“用户-角色”映射机制的 RBAC96 模型，以及衍生出的 ARBAC97 模型和 ARBAC99 模型；随着基于属性的访问控制（ABAC, attribute based access control）[8]类型的出现，ABAC 模型所有请求操作和策略描述均通过属性集传递，有 $ABAC_0$ 模型和 ABACa 模型等代表模型[9-10]。

经过近半个多世纪的研究和发展，为了适应在分布式系统、云计算、移动互联网等不同场景下对客体（资源）的访问控制，出现了一系列新型访问控制模型。针对多域间协同工作特征，面向分布式协同、依赖授权机制和信任管理实现资源的细粒度访问控制，代表模型有使用控制（UCON, usage control）模型、dRBAC 模型等[11-12]；基于任务的访问控制（TBAC, task based access control）模型则从工作流任务的角度建立，在多任务处理的同时提供动态实时的安全策略，代表模型有 Petri TBAC 模型、基于任务-角色的访问控制（T-RBAC, task role based access control）模型等[13]；时空关联的访问控制基于用户所处的时间和空间等要素，通过时态约束和位置约束进行授权决策，代表模型有基于时间-角色的访问控制（TRBAC, temporal role based access control）模型、基于广义时间-角色的访问控制（GTRBAC, generalized temporal role based access control）模型、基于位置的访问控制（LBAC, location-base access control）模型、基于空间位置-角色的访问控制（GEO-RBAC, geospatial role based access control）模型等[14-15]；基于行为的访问控制（ABAC, action based access control）模型在综合角色、时态和环境状态要素的同时，从行为角度建立安全模型，代表模型有基于行为的云计算访问控制安全模型（CCACSM, cloud computing access control security model）、基于行为的多级安全访问控制（AMAC, action-based multilevel access control）模型等[11, 16]。

上述访问控制模型主要适用于集中式、面向特定场景的“有界”单一域，无法满足面向 5G、大数据、物联网等泛在、复杂、“无界”环境下跨域数据资源的动态按需与受控共享需求。为此，工业界和学术界聚焦数据跨域流动过程中的细粒度动态授权与全生命周期可控可管新挑战，数据跨域流通访问控制领域研究只是初现端倪，很多问题尚未提出并解决。本文聚焦面向数据跨域安全流通的访问控制机制，对数据跨域安全流通中的访问控制技术进行了全面综述，如图 1 所示。本文主要研究工作如下。

1) 本文对数据跨域访问控制面临的主要问题进行了明确，包括数据跨域流通基本概念、数据跨域访问控制内涵等。

2) 系统综述了面向数据跨域流通的访问控制

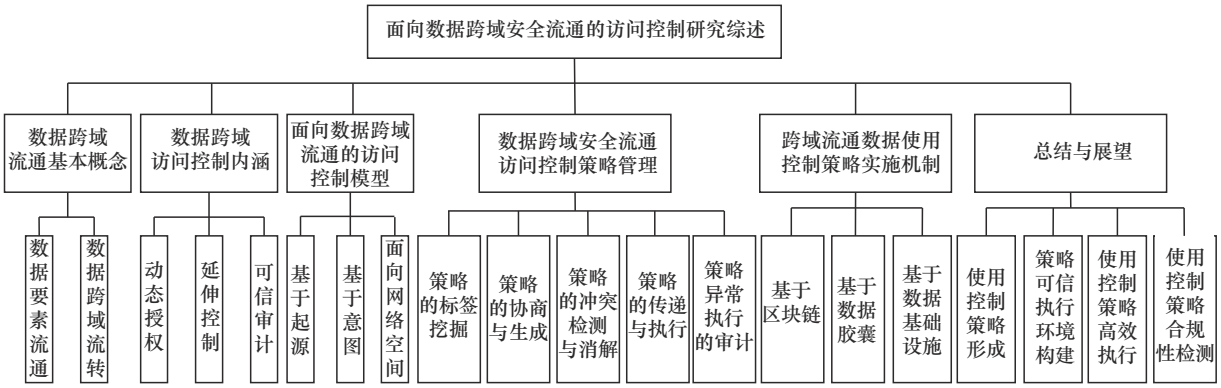


图1 本文研究综述架构

模型，包括基于起源的访问控制（PBAC, provenance based access control）、基于意图的访问控制和面向网络空间的访问控制等模型。

3) 针对跨域安全流通中的数据使用访问控制策略管理，对策略的标签挖掘、策略的协商与生成、策略的冲突检测与消解、策略的传递与执行、策略异常执行的审计等关键技术进行了全面综述。

4) 在面向数据跨域流通的访问控制模型基础上，对结合区块链、数据胶囊、数据基础设施等新技术构建的策略实施机制进行了梳理总结。

5) 最后，对数据跨域安全流通面临的数据使用控制策略形成、策略可信执行环境（TEE, trusted execution environment）构建、使用控制策略高效执行、使用控制策略合规性检测等挑战和问题进行了总结和展望。

1 数据跨域访问控制面临的问题

数据跨域流通能够有效打破单一域信息孤岛、数据壁垒、数据烟囱等现象。然而，由于不同域授权机制的差异，不同来源的敏感数据和个人隐私信息会在不同信息系统中留存，从而产生新的被篡改、被泄露和被滥用的数据安全风险。

1.1 数据跨域流通基本概念

数据要素安全有序流通是数字经济高质量发展的内在驱动力，也是一个国际性难题，尚处于探索阶段。笔者所在团队认为：数据要素是指将原始数据通过加工整理、确权，使其成为具备潜在利用价值的数据资产，并通过在市场上交易流通，让这些数据资产成为可用于社会生产经营活动，能够推动社会生产力发展，并为使用者带来经济效益的重要生产要素。

1.1.1 数据要素流通

数据要素流通[17]是指将数据作为产品进行分类定价、流通和买卖，是数据要素价值和作用发挥的重要途径，包括数据的确权、交易、使用及监测等环节。数据要素流通的市场环境涉及数据供需、数据安全、数据授权和数据交易规则等多方面因素。作为经济管理领域专业术语，数据要素化流通[18]是经济管理、计算机技术和法律制度等多个领域的融合交叉概念，可抽象为一种伴随着价值传递、安全信任传递的数据资源在提供方和需求方之间的交换与转移过程，通常有数据开放、数据共享、数据交易和数据交换等多种数据流通方式。

1.1.2 数据跨域流转

ISO/IEC 18028-3标准[19]最早定义了安全域的概念：即具有相同安全需求的一组资产和资源的集合；同一安全域内部具有相同安全保护需求，服从相同安全策略。安全域是传统的基于“边界”的网络安全防护理论的基础，安全域内部又可分为信任（安全）域、脆弱信任（安全）域和非信任（安全）域等。安全域内部的信任（安全）域默认可信，脆弱信任（安全）域和非信任（安全）域存在域内资源被篡改、被泄露、被滥用的先天劣势。RFC 1983[20]则定义了管理域的概念：即由单一管理者管辖，多个主机、路由器和互联网组成的集合体；作为独立自治的实体，管理着一组资源，拥有自身的管理权限和访问控制策略。

一个信息系统通常由一个管理域组成，也可划分为多个高度自治的安全域，通过安全域之间互操作实现资源的可信流转与共享交换。在数据跨域访问控制中，域通常是指“运维管理控制域（简称管控域）”，即掌握数据资源的管控实体，通常是特

定的机构或组织，例如企事业单位、政府机构等。以数据交换和数据共享为例，数据资源的跨域流通势必造成其所有权和使用权分离，使得原本基于安全域“边界”访问控制模型无法有效保护已经流转到外部的数据资源；同时，对于已交换和共享的数据资源也无法进行延伸授权与管控。因此，面向数据跨域安全流通的访问控制必须打破传统安全域“边界”内部控制，突出以数据资源流动为核心、跨不同主体的管控域内外协同控制理念。值得说明的是，本文讨论的跨域既包含一个管控域内部数据资源传输流转与共享交换（域内关系），也包括多个管控域之间数据资源安全流通与协同应用（域间关系）。

1.2　数据跨域访问控制内涵

复杂环境下，大型应用信息系统通常由多个分布式子系统组成，数据需要在各子系统间频繁流通、共享与交换；而各子系统往往分属不同的安全域、管理域和所在地域，数据在不同实体、系统和管控域之间流通形成数据流；如何实现数据跨域流通过程中，对数据使用的细粒度动态授权与全生命周期管控是数据跨域安全流通面临的主要挑战。因此，面向数据跨域安全流通的访问控制内涵在于：强调数据操作、传播、共享、交换、交易、留存、销毁等层面的管理控制；本质是细粒度的数据使用控制策略如何动态可信执行的问题；重点保证数据资源的机密性管控、完整性管控和有效性管控；避免数据资源被窃取或者非预期地使用。具体而言，面向数据跨域流通的访问控制需要解决动态授权、延伸控制（ECON, extended control）和可信审计等方面的难题。

1.2.1　动态授权

面向数据跨域流通的访问控制动态授权包括跨域用户身份合法性动态验证和数据资源跨域访问细粒度动态授权。其中，跨域用户身份合法性动态验证包括主体对客体的识别以及客体对主体的检验与确认，通过合理地设定控制规则集合，确保跨域认证用户对流转、共享和交换的数据资源在授权范围内的合法使用。一般而言，每个域内都存在一个或多个属性映射函数，用来实现域内属性与全局属性映射。云计算、物联网环境下的数据资源跨域访问细粒度动态授权往往基于域间权限认证与授权单元，或统一认证与授权单元，其实现方式主要有委托机制、域间映射机制和策略集成机制等[21-23]。

数据资源跨域访问细粒度动态授权通常采用域间映射机制，即在域间通过协商方式对各域内主体以一定映射方式进行关联，通过这种映射机制，建立起2个域之间身份与权限信息的映射转换，从而完成跨域授权。以X域数据资源流转到Y域为例，首先调用X域的属性映射函数，将X域内属性映射为全局属性，当X域数据流转共享到Y域时，再调用Y域的属性映射函数，将全局属性映射为Y域的域内属性，从而实现X域到Y域的属性映射。

1.2.2　延伸控制

面向数据跨域流通的延伸控制是指数据资源在跨域受控交换过程中全生命周期各环节隐私操作的迭代控制，以及控制策略的动态调整和可控传递等[24]。延伸控制根据数据提供方的控制意图、当前使用者控制约束和数据接收者的保护能力生成控制策略，使其随数据流转过程同步传递且不可分割，并根据使用场景、延伸控制要求不断动态变化并向前可信可控传递，从而实现迭代控制直至数据的所有副本销毁为止。

1.2.3　可信审计

面向数据跨域流通的可信审计是指按照一定的规则根据跨域用户的访问权限对数据资源流转、共享与交换行为或活动的记录进行检查验证，决定日志中记载的数据资源访问信息是否符合访问策略的过程。控制策略执行的可信审计策略项应与日志格式定义相对应，审计过程和结果以审计记录形式生成并存储于审计库中，通过识别与分析策略异常执行记录保障数据可信，确保存储和传输数据的机密性、防篡改、不可否认性，以及计算的可控性。

2　面向数据跨域流通的访问控制模型

本节系统综述了面向数据跨域流通的访问控制模型，包括基于起源的访问控制、基于意图的访问控制和面向网络空间的访问控制（CoAC, cyberspace-oriented access control）等基础模型。

2.1　基于起源的访问控制模型

在进行数据分析和应用的过程中，企业或组织通常需要对原始数据进行加工和处理，自然而然产生大量衍生数据，但衍生数据难以判断其来源，并且缺乏一种有效的机制确定其使用策略。因此，起源数据通常用来跟踪、记录数据生成过程，即记录谁在何种条件下对数据进行了何种操作，它根据事务中涉及的实

体之间的潜在因果依赖关系形成有向无环图（DAG, directed acyclic graph），基于起源的访问控制模型应运而生。其主要思想是将起源数据当作一种特殊属性来控制对跨域数据对象的访问，从而实现数据资源跨域流转中的访问控制。Park和Nguyen等[25-26]最早联合给出了基于起源的访问控制模型的基本定义、形式化语言和实施框架，如图2所示。

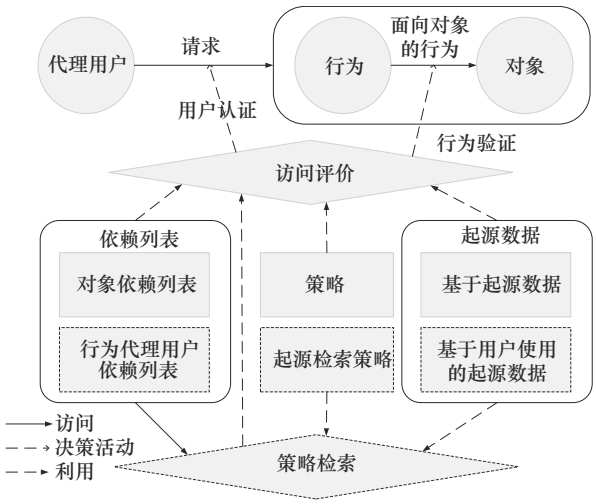


图2　基于起源的访问控制模型

Nguyen等[27]在PBAC模型基础上又提出了$PBAC_B$和$PBAC_C$增强模型，通过扩展来源数据模型和$PBAC_B$模型来强制执行文献[27]中确定的各种动态职责分离（DSOD, dynamic separation of duties）策略类，并超越这些来指定新的DSOD策略类。文献[28-31]在PBAC基础上，分别扩展出基于跨域授权起源的访问控制（DPBAC, delegation provenance based access control）模型，基于PBAC模型的起源感知策略控制框架，ABAC的PBAC访问控制策略框架，以及基于起源的分层加密（PBHE, provenance based hierarchical encryption）机制。文献[32]则提出了一种基于起源的数据流控制（PDFC, provenance based data flow control）机制，该机制实现了对数据流的直接和间接控制，包括跨域流控制和跨域流后进一步控制，并给出了一种记录源数据与其源数据之间关系的源树，可以解决物联网中细粒度可控共享问题。上述工作较好地解决了动态授权与延伸控制部分问题，但未考虑可信审计，因此不能做到对数据非授权操作的溯源。

2.2　基于意图的访问控制模型

传统的访问控制模型不是为了数据资源流通和执行隐私策略而设计的，尤其是带有目的的策略往往是动态环境下跨系统、跨网络传递执行，因此不能满足跨域数据流通和隐私保护要求。Byun等[33]率先提出了基于意图的访问控制（PBAC, purpose based access control）模型，如图3所示。

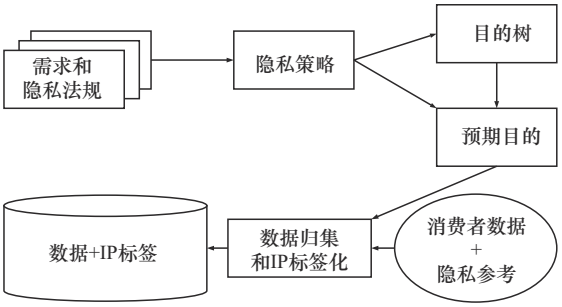


图3　基于意图的访问控制模型

PBAC模型的提出最初源于目的描述思想，该描述详细定义了跨域数据收集、访问和使用的意图，通过构建目的树来清晰表示2个意图之间的层次关系，这一思想同样在经济合作与发展组织（OECD, organization for economic cooperation and development）隐私保护与个人信息流指南中提出[34]。文献[35-39]在基于角色参与的隐私保护基础上，提出了基于意图的动态访问控制（DPBAC, dynamic purpose based access control）模型，基于角色意图的访问控制（RPAC, role-involved purpose based access control）模型，基于条件意图的访问控制（CPBAC, conditional purpose based access control）模型，以及基于角色的条件意图访问控制（RCPBAC, role-involved conditional purpose based access control）模型；上述模型允许用户将某些数据用于有条件的特定目的，从而实现跨安全域的细粒度的隐私保护，但未考虑数据流通场景下跨管理域的基于意图的策略实施。

以数据流通隐私保护场景为例，如表1所示，文献[40-43]分别在PBAC模型基础上，利用不同访问控制方法实现跨域隐私保护机制。上述文献较好地解决了跨域隐私保护问题，但不适用于数据资源共享交换、数据交易等场景，无法解决延伸策略绑定、共享过程监测、异常共享溯源等数据全生命周期可管可控问题。

2.3　面向网络空间的访问控制模型

随着移动互联网、5G通信技术等广泛应用，基于起源的访问控制模型和基于意图的访问控制模

表 1　　基于 PBAC 模型跨域隐私保护实现机制比较

方法	分类	实现机制
结合基于 Petri 网建模方法[40]	基于角色	通过建模的工作流来指定意图的策略实施，以避免泄露隐私数据
将基于属性的访问控制模型和基于意图的隐私模型组合[41]	基于属性	当请求者的属性证书和上下文条件符合服务提供者指定的访问控制策略，同时请求者的隐私首选项与服务提供者的隐私策略兼容，则允许对服务的跨域访问请求
大数据聚类方法[42]	基于属性	基于集群意图的跨域访问控制方法，通过对大数据环境下的大数据集进行聚类，并且只允许授权用户访问
区块链技术[43]	基于角色	基于三重主体意图不同目的和角色的访问控制，实现医疗物联网场景中以个人为中心的跨域隐私保护机制

型，均无法很好地描述用户在多网融合和复杂网络环境访问时所处环境、时态的变化对权限描述和授权管理的影响。为此，在综合角色、时态和环境状态等相关安全信息的同时，2008 年 Li 等[44]引入“行为”概念，提出了基于行为的访问控制模型，该模型[45-46]描述了角色、时态和环境之间的关联关系，并对行为状态管理函数进行了形式化描述；针对跨域协作信息系统资源授权的决策问题，给出了相应的安全关联描述、产生方法以及一种安全认证协议，并设计了一种 ABAC 模型应用于 Web 服务的安全体系结构。文献[47]以多级安全模型为参考，对 ABAC 模型进行了扩充，提出了一种基于行为的云计算访问控制安全模型（CCACSM, cloud computing access control security model），该模型兼顾了用户所处的环境和时态要素，能够解决云计算环境下的机密性和完整性问题。文献[48-49]针对数据分级化管理问题，将多级安全与基于行为的访问控制相结合，提出了具有时间限制和约束特征的多级安全访问控制、基于行为的结构化文档多级安全访问控制等模型，并进行了形式化描述。

李凤华等[50]提出了面向网络空间的访问控制模型，该模型由访问请求实体、网络/广义网络及资源（集合）3 部分组成。如图 4 所示，访问请求实体（集合）Q（即资源访问的发起方）发起对相应资源（集合）O（即访问的对象及其相关属性）的访问请求；该请求经由广义网络（集合）N（即信息传播的载体）到达资源服务器；资源服务器将 Q 在生产访问请求中所使用设备（集合）D、广义时态（集合）T、接入点（集合）L 等信息与既定访问控制策略进行匹配；若匹配成功，则将 O 通过 N 返回给 Q；若匹配不成功，资源服务器将拒绝 Q 对 O 的访问。该模型本质是网络接入的访问控制与信息系统的授权/鉴权进行关联，实现泛在接入场景下细粒度控制。该模型可有效防止因数据所有权与管理权分离、信息再次/多次转发等带来的安全问题，其中，信息的再次/多次转发控制又被称为

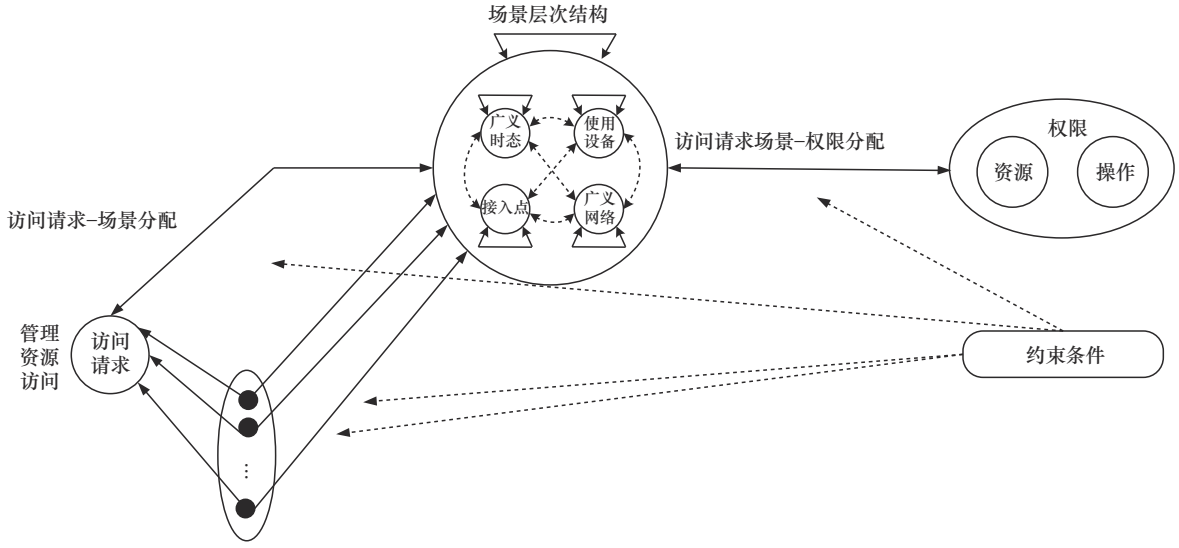


图 4　面向网络空间的访问控制模型

延伸控制。

表2为基于CoAC模型延伸控制实现机制比较，文献[51-53]分别在CoAC模型基础上，实现了不同场景下信息的细粒度延伸控制。

3 数据跨域安全流通访问控制策略管理

数据跨域安全流通过程中，数据使用控制策略管理是保障细粒度动态授权、全生命周期访问控制的基础，主要包括策略的标签挖掘、策略的协商与生成、策略的冲突检测与消解、策略的传递与执行，以及策略异常执行的审计等方面。

3.1 策略的标签挖掘

为了更好地管理跨域流通数据，需要对跨域数据本身进行标记处理和内容分析，通过文本挖掘和主题提取为每个流转信息产生标签建立索引，使数据分类明确，从而提高检索效率。

访问控制的数据标签挖掘技术最早源于BLP模型，用于数据细粒度自动标记与策略生成。基于数据标签挖掘技术的数据跨域策略管理即采用标签补全、标签发现和标签排序等技术，将跨域数据与其密级、分类、共享范围等安全控制信息相结合，基于标签属性进行细粒度的授权与控制，实现包括结构化和非结构化数据按语义自动细粒度标记、分级标签自动融合等功能。文献[54-55]分别通过分配隐私策略标签和共享数据策略标签，在满足发布信息和共享数据细粒度访问控制的同时，实现用户隐私保护和非法共享数据的起源追踪。

3.2 策略的协商与生成

作为应用最广泛的跨域访问控制模型，基于互操作性角色的访问控制（IRBAC, interoperability role based access control）2000模型[56]基于域内用户静态角色属性，尽管能实现域间角色的关联映射，但不能实施域间动态授权和权限即时回收，不具备权限自动调整能力。现有的跨域策略协商理论和方法可以按照多种角度分类，例如，从协商主体、协商对策、协商主题等角度。从协商主体的理性决策方面看，现有用于使用策略协商的方法大致分为两类：基于非博弈的协商和基于博弈的协商。现有的协商机制忽视了使用条件和义务，也不能实现权限的动态优化和策略的自调整。因此，国内外研究者在基于属性的动态授权基础上，进行了大量的创新，如表3所示。

访问控制策略作为访问控制鉴权的核心依据之一，现有的策略生成技术则包括两类：自顶向下方法和自底向上方法，但不能直接应用于跨域延伸控制策略的协商。

3.3 策略的冲突检测与消解

数据跨域流通导致访问控制策略数量庞大，策略内或策略间易发生冲突，因此，策略的冲突检测与消解对于保证策略的正确性尤为重要。策略的冲突检测与消解主要指域间策略生成决策与指令分发过程中的冲突自动检测和快速消解。

早期，策略的冲突检测与消解主要以可扩展的访问控制标记语言（XACML, eXtensible access con-

表2 基于CoAC模型延伸控制实现机制比较

参考文献	管理场景	实现机制
文献[51]	电子发票全生命周期控制	提出基于起源信息的约束控制和传播控制授权机制
文献[52]	社交网络隐私保护	提出基于传播链的跨社交网络的隐私图片分享框架
文献[53]	社交网络隐私保护	提出基于用户关系跳数和资源转发跳数给用户和数据分配不同类型的隐私标签，实现数据细粒度延伸控制

表3 基于属性的跨域策略协商与生成实现机制比较

方法	分类	实现机制
基于风险或时间的权限自适应[57-58]	基于算法	当风险小于预定阈值或在超出预定时间域时，系统自动检测撤销或调整已分配权限
基于FairAccess机制[59]	基于算法	利用机器学习算法改进访问控制策略，实现权限的动态优化和自调整的策略
结合ABAC模型和区块链技术[60-61]	基于区块链	结合ABAC模型，分别实现基于区块链代币机制和布隆过滤器（BF, Bloom filter）的策略查询、访问权限动态判决和更新，从而满足动态访问控制需求
基于密钥策略的属性加密[62]	基于密码学	基于密钥策略的属性加密（KP-ABE, key-policy attribute based encryption）用户关系动态机制，实现云计算环境下访问控制策略的自动更改

trol markup language）编写的策略转化为决策图的方法[63-64]，随后出现了用描述逻辑（DL, description logic）进行了形式化定义的XACML2.0和国际标准XACML3.0，使用多终端二进制决策图作为底层机制，分析属性缺失情况下的策略变更，也可用于分析不同策略之间的语义差异。该机制通过将云服务策略转换为XACML策略，设计了基于多终端多数据类型区间决策图（MTMIDD, multi-terminal multi-data-type interval decision diagram）和扩展MTMIDD（X-MTMIDD, eXtended MTMIDD）的XACML策略表示和异构策略间冲突搜索方案，为了降低误报率，使用DL来表示XACML策略并消除假冲突。此外，常见的基于有向图、决策图、特殊矩阵等模型的安全策略冲突检测方法往往同XACML结合使用。

随着访问控制技术在移动互联、云计算、物联网场景中不断应用，出现了一系列策略的冲突检测与消解新方法，如表4所示。

3.4　策略的传递与执行

策略的传递与执行指数据跨域流通过程中，对数据资源的访问进行实时控制和管理时，策略本身的精确传递与可信执行，目的是确保数据资源和控制策略在传输过程中不被未经授权的访问或篡改。信息流控制技术可以限制信息在单域系统中的流动，从而确保策略的强制执行，但不适用于数据跨域流通。

跨域访问控制策略的传递与执行实现机制[68-74]比较如表5所示，本文认为跨域访问控制策略的传递与执行主要有以下2种类型。

1) 分离式

针对原始数据和衍生数据，跨域流通时数据资源文件和策略文件同时流转，形成数据流与控制流，策略与数据分离式传递与执行。

2) 绑定式

访问控制策略与数据本身绑定在一起，策略与数据绑定式传递与执行，其核心思想黏性策略（SP, sticky policy）最早由Karjoth等[75]提出。

总而言之，策略与数据分离式传递与执行始终存在对数据的控制粒度不够细问题；而绑定式传递与执行则可以根据不同的数据类型和应用场景，为每个数据实例分配不同的使用规则，从而实现对跨域数据访问的动态控制。相比传统的分离式传递与执行基于角色或属性的访问控制方法，绑定式传递与执行更加灵活、细粒度，并且能够适应大规模、互联和分布式系统等复杂环境下的需求。

3.5　策略异常执行的审计

策略异常执行的审计是一种操作行为事后认定违反既定访问控制策略的跟踪分析技术，可通过跟踪查询、分析、挖掘审计日志，实现对角色或属性

表4　复杂网络环境策略的冲突检测与消解实现机制比较

方法	管理场景	实现机制
基于多目标整数规划优化的跨域访问控制策略映射机制[65]	移动互联	将最大化域间互操作性和最小化域内自治性作为目标函数，将7类典型的跨域冲突作为约束函数，设计了一种带约束的多目标优化非支配排序遗传Ⅲ算法（NSGA-Ⅲ, nondominated sorting genetic algorithm Ⅲ），从而实现平衡域间互操作性和域内自治性
基于监测设备状态和行为策略[66]	物联网场景	通过监测物联网批量设备状态和触发器的行为策略，编码实现物联网监测系统（IoTGUARD），能够保证应用策略冲突的动态检测与处置
基于主体信任惩罚度和信任度属性[67]	云计算	利用Hicuts算法对策略进行分类，降低冲突检测的数量，提高冲突检测的效率；对于存在冲突的访问控制策略，根据冲突类型进行相应的消解，依据算子设计原则、主体信任度和策略相似性进行决策

表5　跨域访问控制策略的传递与执行实现机制比较

方法	分类	实现机制
基于文件访问控制系统[68-69]	分离式	分别编码实现文件访问控制系统LoNet和Zeph，每个流转文件都有对应的策略文件，解析并执行不同需求和隐私策略，以实现处理多种来源的数据流
基于进程的管道控制[70-71]	分离式	2种类型的策略分别作用于原始数据和衍生数据的管道进程：一种是标准访问策略（读或写），作用于限制边界外的进程（非受限进程）；另一种是解密策略（写），作用于限制边界内的进程（受限进程）；模拟的仿真环境去评估不同域之间策略的相似度，以及不同域之间策略规则的可映射度，以及有多少策略规则需要手动编码来部署，解决了跨域边界执行策略的难题
基于密码学[72-74]	绑定式	将数据和策略绑定后一起加密传输，利用属性编码和匿名化处理等技术以防止策略被恶意利用，实现数据全生命周期受控流转

创建与删除、权限修改、关系映射等访问控制策略异常的审计。

文献[76]提出了一种基于区块链的可溯源访问控制机制，该机制将访问控制策略以智能合约的形式部署在区块链上，将访问授权日志和访问日志记录在日志区块链上，通过日志区块链实现跨域访问授权和全过程的可审计、可追踪和可溯源。Xiang等[77]提出了一种新的时变决策树（TCDT, time-changing decision tree）结构和学习算法，可以从访问日志中自动推断访问策略更改，并实现了一种持续监视访问日志的实用工具P-DIFF，该工具可以帮助系统管理员检测异常的访问控制策略更改，并帮助识别已知安全事件的历史策略变改。针对数据在跨域传播过程不透明的问题，笔者所在团队提出了面向数据跨域流通的资源传播链构造方法[51,53,65]，实现数据异常共享的审计与溯源；该方法可通过基于文本相似度的日志补全等方式，分析数据的传播源、中继节点、目的节点、操作者及其操作时序关系，实现资源传播构造的细粒度还原。

4　跨域流通数据使用控制策略实施机制

工业界现有常见的跨域数据控制方案，由于存在控制粒度不够细、数据所有者无法自定义对数据的使用策略、缺少权限和策略的分配、策略异常执行审计等问题，无法实现对非授权数据操作的溯源，也无法抽象成为典型的跨域访问控制模型。因此，学术界在面向数据跨域共享交换的访问控制模型基础上，结合区块链、数据胶囊、数联网、数据空间和数据组件等新技术、新方法尝试构建典型数据使用控制策略实施机制。

4.1　基于区块链的策略实施机制

身份认证与授权框架下跨域访问协议通常有Kerberos、Passport、安全断言标记语言（SAML）等，用来解决第三方可信代理问题。如图5所示，随着访问控制技术与区块链技术的深度融合，基于区块链“去中心化”信任关系来实现跨域身份认证与授权新机制应运而生。

面向数据跨域流通场景，基于区块链的访问控制策略实施机制主要有基于交易事务、基于智能合约、基于密码学与区块链访问令牌机制等类型。如表6所示，分类展示了不同类型的基于区块链的策略实施代表机制的主要思想。

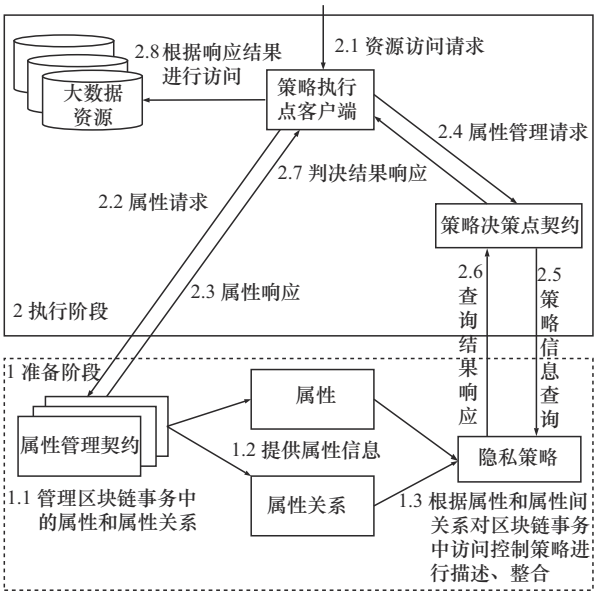


图5　基于区块链的策略实施机制

1) 基于交易事务

借助区块链的可信存储特性，将策略、主体和客体信息及日志等数据打包，并以事务交易形式存储到区块链中，其代表机制有Maesa机制[60]、Zyskind机制[78]、控制链（ControlChain）机制[79]等。

2) 基于智能合约

借助区块链的可信计算特性，将策略转化为智能合约代码并上传至区块链，自动化地赋予其对客体的访问权限，代表机制有基于区块链的分布式大数据访问控制（BBAC-BD）机制[61]、使用智能合约基于角色的访问控制（RBAC-SC）机制[80-82]、基于区块链的医疗记录访问控制（MedRec）机制[83-84]等。

3) 基于密码学与区块链访问令牌机制

针对数据资源跨域流转中难以管理的问题，引入公钥密码学，通过公钥证书[85-86]、Token访问令牌[87]等识别用户，以安全的方式为内容提供者提供内容的共享、审计和撤销能力，同时可抵抗单点故障，代表机制有分散式在线社交网络场景下的分散式在线社交网络（DOSN）机制。

总而言之，基于区块链的策略实施机制具有去中心化、数据透明和防篡改等显著优点，适用于对安全性和信任要求较高的应用场景。然而，其缺点也较为明显，包括执行性能问题、隐私泄露风险，以及智能合约的安全性和成本问题等。

表6　基于区块链的策略实施机制比较

方法	分类	主要思想
BBAC-BD机制[61]	基于智能合约	基于ABAC模型与区块链技术相结合，通过区块链事务管理访问控制策略及属性，策略以公开、透明的形式存放在区块链中，通过智能合约，基于资源拥有者发布到区块链上的策略，实现对大数据资源自动化的访问控制
Zyskind机制[78]	基于交易事务	在区块链等分布式网络中利用零知识证明和安全多方计算技术来保护跨域数据的隐私，以实现在不泄露任何实际数据的情况下进行验证和计算
ControlChain机制[79]	基于交易事务	通过链上存储访问控制权限、策略、关键敏感数据和操作记录等，使得认证用户无法撤销对其数据的授权访问，从而实现以区块链作为可信第三方来防止数据被篡改，多应用于云计算、物联网等场景
RBAC-SC机制[80-82]	基于智能合约	基于属性的访问控制策略编码为智能合约，基于组的策略扩展，利用许可的区块链实现以安全、可审计的方式分发访问控制策略，同时保持每个组织的独立性
MedRec机制[83-84]	基于智能合约	通过与访问控制相结合，支持用户信息管理、链上数据管理、数据整合与查询、违规行为监测和访问权限判决等细粒度控制，该机制可应用于电子病历、云监控等场景
DOSN机制[85-87]	基于密码学域区块链访问令牌机制	分散式在线社交网络场景，使用公钥证书识别用户，区块链则定义隐私策略，资源所有者使用主体的公钥用于访问控制列表定义可审计的访问控制策略，而与主体的Ethereum账户关联的私钥用于在区块链上验证访问权限后解密私有数据

4.2　基于数据胶囊的策略实施机制

Maniatis等[88]最早提出了数据胶囊的概念，即数据胶囊由数据、使用策略和来源组成，数据基于黏性策略以数据胶囊的形式进行加密传播。如图6所示，基于数据胶囊的策略实施机制的主要思想是：当用户想要访问数据时，首先会进行身份验证，验证通过后由胶囊管理器对用户的请求进行评估，如果评估结果是允许，则会解密数据胶囊并通过安全通道传输给安全的执行环境。

文献[89-90]提出数据与策略绑定的数据胶囊范式，用于处理异构数据基础设施中数据隐私法规的自动合规性检查，该范式的核心思想是将数据主体与控制数据处理方式的策略绑定，使得策略由数据主体与数据一起创建和提供，并在数据处理的整个生命周期（例如，数据处理系统的数据转换、多个数据主体数据的数据聚合过程）中与数据始终相关

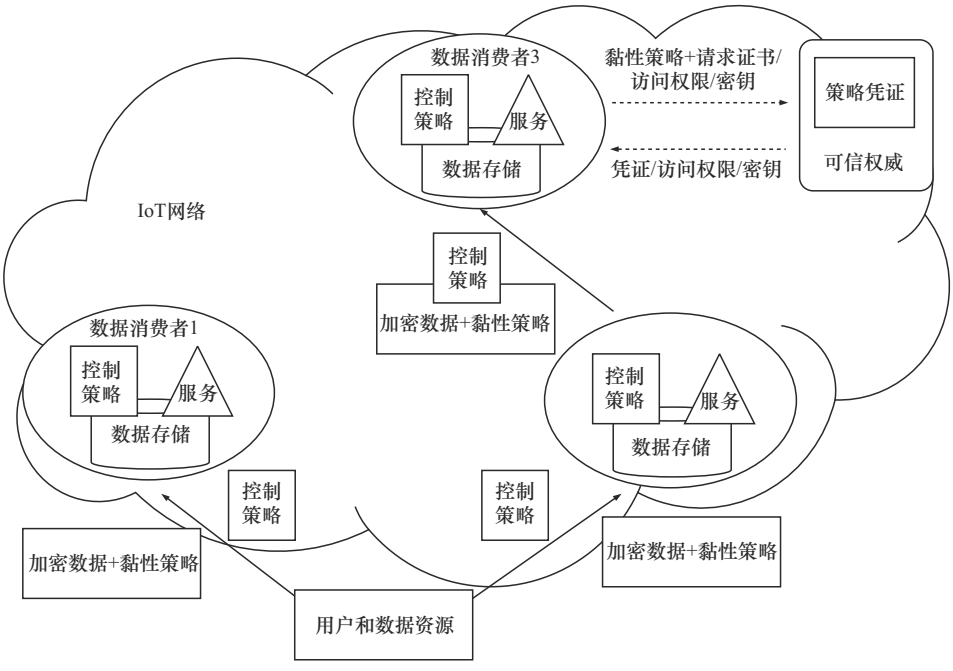


图6　基于数据胶囊的策略实施机制

联；同时，该范式提出了一种基于剩余策略概念的静态执行隐私策略的解决方案，以及一种基于抽象解释的私有策略中剩余策略新算法。同时，在数据胶囊范式基础上，通过使用抽象解释的静态分析方法实现了一个检测程序合规性的原型系统（PRIVGUARD），并提出了一种编码隐私策略的形式化语言（PRIVPOLICY），该系统的输入是隐私策略和一段待检测的程序，输出是未被满足的隐私策略，以提高合规过程的生产率和减少人工参与。

基于数据胶囊的数据使用控制策略实施机制通过封装技术来允许控制数据在不可信环境中的使用，并确保数据使用符合既定的安全策略，其主要优势在于与数据高度耦合的安全控制和策略的自动执行，同时能够动态适应数据使用场景的变化；其缺点是数据在传播的过程中会记录其来源，产生的衍生数据会同样执行原始数据的使用策略，以及在数据胶囊转发的过程中无法高效地追踪信息流并且缺乏有效的隔离机制。

4.3 基于数据基础设施的策略实施机制

当前，学术界对数据基础设施并没有统一的定义。广义来说，数据基础设施是从数据要素价值释放的角度出发，是集成硬件、软件、模型算法、开源协议、标准规范、机制设计等在内的有机整体；狭义而言，数据基础设施是数据全生命周期的技术和工具，技术实现方式通常包括基于数联网、基于数据空间和基于数据组件等。

4.3.1 基于数联网

数联网[91-93]即数据互联网，指在物联网和数字对象架构（DOA, digital object architecture）基础上，采用软件定义网络思路，通过以数据为中心的开放式软件体系结构和标准化互操作协议，将各种异构数据平台和系统相连接，从而构建形成人机物融合的虚拟网络。

基于数联网的策略实施主要包括跨域数字身份认证和跨域数据使用控制。其中，跨域数据使用控制主要包括事前策略在线协商、事中设备层与数据应用APP访问策略控制、事后日志存证与审计等。文献[94-95]基于标识解析技术，设计实现面向人机物融合的数联网数字对象标识原型系统，可根据不同的网络拓扑结构以及应用场景配置合适的标识解析策略，解决数据资源共享交换过程安全管控难问题。文献[96]基于时空码和数联网技术，将数据放入“空间+对象”融合框架“容器”，面向数据流通厂家，针对每一个数据对象建立了完整的时空轨迹流通链，针对全局实现了全时空全要素全状态的大数据组织，支撑全量数据流通轨迹的高效搜索与计算。

4.3.2 基于数据空间

面向数据流通领域的数据空间概念源于国际数据空间协会（IDSA, international data space association）提出的国际数据空间（IDS, international data space）[97]理论，我国在此基础上提出以“跨域数据使用控制”为核心建立可信数据空间（TDM, trusted data matrix）[98]，并与国际组织合作完成了IEEE P3158《可信数据空间系统架构》国际标准，发布了《可信数据空间发展行动计划（2024—2028年）》[99]，将其作为数据要素流通的关键数据基础设施，如图7所示。

基于数据空间的策略实施机制应用场景主要集中在边缘计算、工业物联网、医疗健康和物流等领域。文献[100]参考IDS体系结构将可信数据交换机制集成到多访问边缘计算（MEC, multi-access edge computing）环境中，从而提出IDS连接器即服务的概念，使用IDS连接器组件在MEC应用程序或MEC平台之间进行可信和安全的通信与数据共享交换；文献[101]提出了一种新的工业物联网数据空间参考架构，该架构包括物联网设备层、边缘计算层和云平台层，以及系统监控、资源管理和安全管理等关键模块，以实现工业物联网数据流的高安全性和高可用性流通；文献[102-104]从数据驱动组织和数据生态系统角度，以医疗数据空间、产业供应链数据空间和智慧城市数据空间等应用为例进行了深入分析，明确应采取可信的远程策略实施、可验证的数据跟踪和资源受限参与者的集成等技术措施来保证数据共享和交换安全；文献[105]针对数据空间中连接器重要构成，开发和集成了一个分类算法，以解决数据使用控制策略合规性问题。

4.3.3 基于数据组件

基于数据组件策略实施机制是指对数据进行模块化封装，通过将数据与其元数据、策略、使用权限等绑定在一起，以数据元件、数据件等数据组件为具体实现形式。文献[106-107]提出以数据元件和内外网数据金库为基础形成安全可信数据空间，从而构建全国一体化数据要素安全高效流通体系。文献[108]提出基于数据件（Dataware）构建安全可信

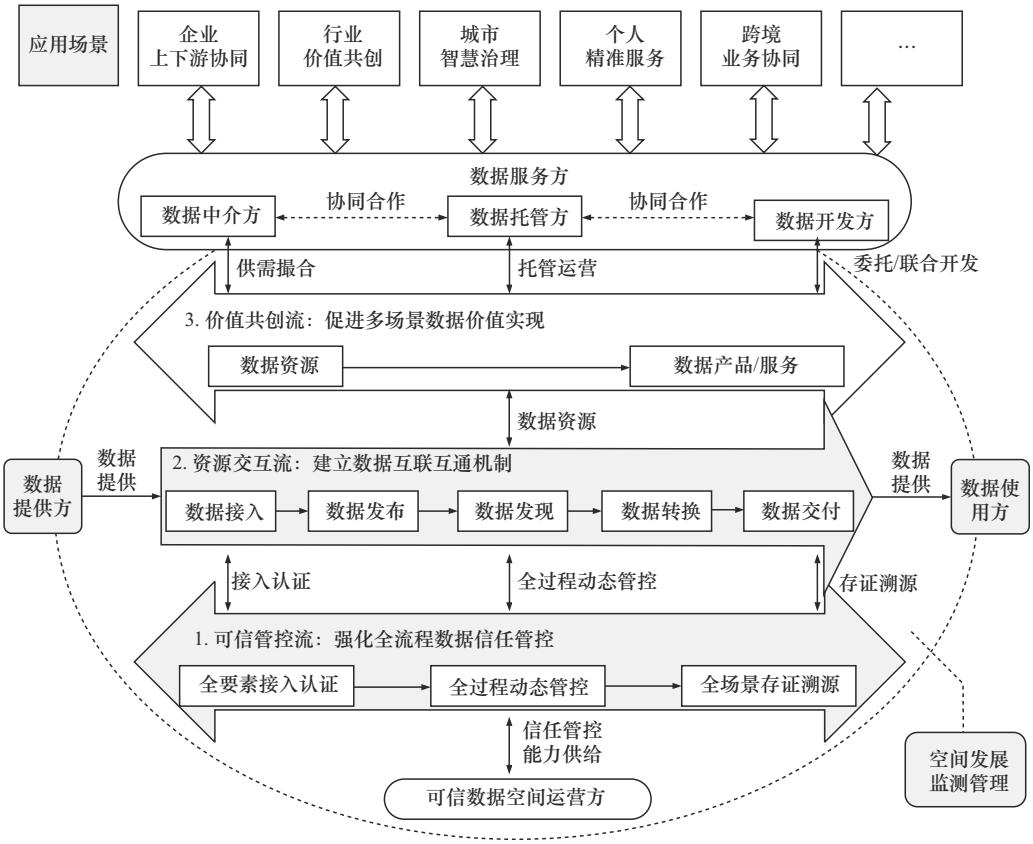


图 7　基于可信数据空间的数据基础设施能力视图

数据空间的管理层和安全层，并将其作为跨域数据基础设施使用控制的核心。

总而言之，基于数据空间的策略实施机制更适合跨组织、跨平台的数据流通与共享；强调去中心化的基于数联网的策略实施机制依托区块链和智能合约技术自动执行访问控制，然而其性能问题和跨境法律合规问题需要解决；基于数据元件、数据件等数据组件的策略实施机制通过将数据与策略封装在一起，实现了数据流通中的自使用控制，增强了安全性和灵活性，但实现成本较高，且面临跨平台兼容性挑战。

5　总结与展望

数据安全作为国家安全的重要组成部分，数据可控是数据资源开放共享、开发利用、流通交易的核心基础。面向数据跨域安全流通的访问控制即通过认证、授权、审计等技术手段控制数据的访问权限，确保数据资源在流通过程中全生命周期的使用可控，包括：访问、加工、删除、脱敏、流转管控、边界过滤、追踪溯源、违规判定、审计、取证等操作的可控。具体而言，在数据流通环境，可以解决泛在传播的权限控制、移动业务的数据使用、多副本完备删除以及全生命周期各操作环节的使用情况存证与合规审计等问题；在终端领域，数据受控共享、交换流转能够支撑发起者的数据确权。数据资源访问控制技术已成为数据跨域流转过程中，保障数据要素的安全流通共享与协同应用的核心技术。传统的单域访问控制模型和域间静态授权与控制机制，已经无法适用于复杂环境中的数据跨域流通场景，主要面临以下挑战。

5.1　使用控制策略形成

数据跨域流通涉及数据所有权、管理权、使用权、收益权等权属的转移，数据确权用于界定数据资源的权属，是数据交易的前提，支撑数据资产入表。数据跨域流通不改变数据所有权和管理权，使用控制策略的形成面临符合数据使用权交易，限定数据接收方按契约使用，控制数据使用范围，约束二次传播，解决使用控制的远程验证问题等一系列挑战。未来，数据跨域使用控制应采用交易契约关联的数据使用策略、数据使用策略与数据资源安全绑定等技术措施，使用控制

策略形成应考虑数据使用者使用数据的条件、数据使用者的权限和义务等因素，确保数据要素跨域流通受控使用。

5.2 策略可信执行环境构建

现有研究难以支撑跨域控制和延伸控制策略可信环境的构建。在不同的应用场景下，数据跨域流通的方式也会有所不同，可能会导致策略在不可信环境中执行的问题，这成为数据跨域流通环境下受控共享面临的新挑战。例如，在Web应用程序中，数据通常是通过网络传输的，而数据的访问和控制则需要在服务器端进行管理；在安卓系统中，数据可能会存储在本地设备上，并且需要通过应用程序进行管理和控制；而在检索系统中，数据通常是从不同的源获取的，并且需要在检索过程中对其进行合并、去重等处理。

目前，学术界和工业界通过借助可信执行环境，在计算平台上由软硬件方法构建的安全区域内部加载的代码和数据能够在机密性和完整性方面得到保护。同时，无论服务器端、本地端，还是应用程序本身，作为“重量级”的可信执行环境亦能够保证访问控制策略能够可信执行，以确保数据资源在内存中流转的安全和合法使用。因此，数据跨域共享交换可以从硬件、算法、通信、计算方式等多个维度来提升性能，但不能以牺牲安全性的方式来提升性能。未来应进一步研究可信执行环境与云原生安全融合相关技术，通过容器虚拟化隔离技术构建更加安全、轻量级、便于移植的跨域访问控制策略可信执行微环境。

5.3 使用控制策略高效执行

随着移动互联网、物联网、5G等技术的发展，面向数据跨域共享交换的访问控制在企业、个人等用户终端表现得越来越轻量级、小型化，跨域访问控制策略的协商、执行与审计等机制的高效性和易用性不足，因此，还需要进一步提升策略执行效率和性能。目前，学术界有研究者设计了一种基于历史信息的高效点到点策略协商算法，通过同步高频协商策略、存储历史协商信息、计算属性披露开销，来优化协商流程，提高交互效率。未来应集中研究跨域访问控制策略和延伸控制策略在轻、快终端中如何高效执行的问题。

5.4 使用控制策略合规性检测

在严格的数据安全和隐私保护要求下，数据资源的跨域访问必须在遵守法规政策和策略授权的前提下进行。通过在可信环境中进行日志审计和合规性检测，可以有效地降低数据资源被滥用和被泄露的安全风险，保障数据资源的安全和隐私。因此，数据资源访问日志的审计与策略的合规性检测成为控制数据跨域共享交换的重要环节。目前，日志信息存在一定的局限性，主要表现在日志信息的粒度取决于应用程序本身，未来应研究在跨域访问控制中如何实现细粒度日志审计的问题。同时，如何确保跨域访问控制策略准确、正确执行且无异常，也是未来值得深入考虑的问题。

6 结束语

中共中央、国务院《关于构建数据基础制度更好发挥数据要素作用的意见》（又称“数据二十条”）初步搭建了我国数据基础制度体系，明确提出要建立数据来源可确认、使用范围可界定、流通过程可追溯、安全风险可防范的数据可信流通体系。《数字中国建设整体布局规划》明确要求“畅通数据资源大循环”“筑牢可信可控的数字安全屏障”。《“数据要素×”三年行动计划（2024—2026年）》要求发挥数据要素的放大、叠加、倍增作用，“打造安全可信流通环境，探索建设重点行业和领域数据流通平台，增强数据利用可信、可控、可计量能力，促进数据合规高效流通使用，提升数据安全保障水平”。随着国家及地方数据局的相继成立，多个地区开展了数据流通与交易方面的先行先试、探索实践，并陆续出台一系列相关政策法规。当前，数据交易所通常采用事前管控方式，对交易数据产品进行合规性评估，缺乏针对后续交付过程和使用过程的安全管控。因此，只有建立数据跨域安全流通管控保护机制，实现对数据使用的细粒度动态授权与全生命周期管控，才能更好激活数据要素潜能，构建以数据为关键要素的数字经济。

参考文献：

[1] LAMPSON B W. Protection[J]. ACM SIGOPS Operating Systems Review, 1974, 8(1): 18-24.

[2] SANDHU R S, SAMARATI P. Access control: principle and practice[J]. IEEE Communications Magazine, 1994, 32(9): 40-48.

[3] SANDHU R S, COYNE E J, FEINSTEIN H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[4] AMMANN P E, SANDHU R S. Implementing transaction control expressions by checking for absence of access rights[C]//Proceedings of

the Eighth Annual Computer Security Application Conference. Piscataway: IEEE Press, 1992: 131-140.

[5] BELL D E, PADULA L J L. Secure computer system: unified exposition and multics interpretation[R]. 1976 .

[6] BELL D E. Looking back at the bell-La padula model[C]//Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05). Piscataway: IEEE Press, 2005: 337-351.

[7] VITO B L D, PALMQUIST P H, ANDERSON E R, et al. Specification and verification of the ASOS kernel[C]//Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy. Piscataway: IEEE Press, 1990: 61-74.

[8] HU V C, FERRAIOLO D, KUHN R, et al. Guide to attribute based access control (ABAC) definition and considerations[J]. NIST Special Publication, 2013: 1-37.

[9] YUAN E, TONG J. Attributed based access control (ABAC) for web services[C]//Proceedings of the IEEE International Conference on Web Services (ICWS'05). Piscataway: IEEE Press, 2005

[10] JIN X, KRISHNAN R, SANDHU R. A unified attribute-based access control model covering DAC, MAC and RBAC[C]///Proceedings of the Data and Applications Security and Privacy XXVI. Berlin: Springer, 2012: 41-55.

[11] PARK J, SANDHU R, PARK J, et al. Towards usage control models: beyond traditional access control[C]//Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2002: 57-64.

[12] SHAFIQ B, JOSHI J B D, BERTINO E, et al. Secure interoperation in a multidomain environment employing RBAC policies[J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(11): 1557-1577.

[13] KNORR K. Dynamic access control through Petri net workflows[C]// Proceedings of the Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00). Piscataway: IEEE Press, 2000: 159-167.

[14] BERTINO E, BONATTI P A, FERRARI E. TRBAC: a temporal role-based access control model[J]. ACM Transactions on Information and System Security, 2001, 4(3): 191-233.

[15] BERTINO E, CATANIA B, DAMIANI M L, et al. GEO-RBAC: a spatially aware RBAC[C]//Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2005: 29-37.

[16] 初晓博, 秦宇. 一种基于可信计算的分布式使用控制系统[J]. 计算机学报, 2010, 33(1): 93-102.
CHU X B, QIN Y. A distributed usage control system based on trusted computing[J]. Chinese Journal of Computers, 2010, 33(1): 93-102.

[17] 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

[18] 郭兵, 胡誉川, 郑臻哲, 等. 数据流通方式：交换、开放、交易，还是共享？[J]中国计算机学会通讯, 2023, 19(7): 44-47.
GUO B, HU Y C, ZHENG Z Z, et al. How data circulation: Internet change, open, trading, or sharing?[J]. Communications of China Computer Federation, 2023, 19(7): 44-47.

[19] ISO/IEC 18028-3. Information technology security techniques IT network security part 3: securing communications between networks using security gateways[S]. 2005.

[20] RFC 1983. Internet users' glossary[S]. 1996.

[21] 袁家斌, 魏利利, 曾青华. 面向移动终端的云计算跨域访问委托模型[J]. 软件学报, 2013, 24(3): 564-574.
YUAN J B, WEI L L, ZENG Q H. Delegation based cross-domain access control model under cloud computing for mobile terminal[J]. Journal of Software, 2013, 24(3): 564-574.

[22] 李瑞轩, 赵战西, 文坤梅, 等. 基于本体的多域访问控制策略集成研究[J]. 小型微型计算机系统, 2007, 28(9): 1710-1714.
LI R X, ZHAO Z X, WEN K M, et al. Ontology-based integration of multi-domain access control policies[J]. Journal of Chinese Computer Systems, 2007, 28(9): 1710-1714.

[23] PAN L, LIU N, ZI X C. Visualization framework for inter-domain access control policy integration[J]. China Communications, 2013, 10(3): 67-75.

[24] 李凤华, 李晖, 牛犇, 等. 隐私计算的学术内涵与研究趋势[J]. 网络与信息安全学报, 2022, 8(6): 1-8.
LI F H, LI H, NIU B, et al. Academic connotation and research trends of privacy computing[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 1-8.

[25] PARK J, NGUYEN D, SANDHU R. A provenance-based access control model[C]//Proceedings of the 2012 10th Annual International Conference on Privacy, Security and Trust. Piscataway: IEEE Press, 2012: 137-144.

[26] NGUYEN D, PARK J, SANDHU R. Integrated provenance data for access control in group-centric collaboration[C]//Proceedings of the 2012 IEEE 13th International Conference on Information Reuse & Integration (IRI). Piscataway: IEEE Press, 2012: 255-262.

[27] NGUYEN D, PARK J, SANDHU R. A provenance-based access control model for dynamic separation of duties[C]//Proceedings of the 2013 Eleventh Annual Conference on Privacy, Security and Trust. Piscataway: IEEE Press, 2013: 247-256.

[28] MOHY N N, MOKHTAR H M O, EL-SHARKAWI M E. Delegation enabled provenance-based access control model[C]//Proceedings of the 2015 Science and Information Conference (SAI). Piscataway: IEEE Press, 2015: 1374-1379.

[29] ALI M, MOREAU L. A provenance-based policy control framework for cloud services[C]//Provenance and Annotation of Data and Processes. Berlin: Springer, 2015: 127-138.

[30] BERTOLISSI C, DEN HARTOG J, ZANNONE N, et al. Using provenance for secure data fusion in cooperative systems[C]//Proceedings of the 24th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2019: 185-194.

[31] FAN X Y, ZHANG F E, TURAMAT E, et al. Provenance-based hierarchical encryption for fine-grained access control in cloud computing[C]// Proceedings of the 2020 2nd International Conference on Industrial Artificial Intelligence (IAI). Piscataway: IEEE Press, 2020: 1-6.

[32] XIE R N, LI H, SHI G Z, et al. Provenance-based data flow control mechanism for Internet of things[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(5): e3934.

[33] BYUN J W, LI N H. Purpose based access control for privacy protection in relational database systems[J]. The VLDB Journal, 2008, 17(4): 603-619.

[34] Organization for Economic Cooperation and Development. OECD guidelines on the protection of privacy and trans-border flows of personal data of 1980[R].1980.

[35] PENG H C, GU J, YE X J. Dynamic purpose-based access control[C]//

Proceedings of the 2008 IEEE International Symposium on Parallel and Distributed Processing with Applications. Piscataway: IEEE Press, 2008: 695-700.

[36] ENAMUL KABIR M, WANG H, BERTINO E. A conditional purpose-based access control model with dynamic roles[J]. Expert Systems with Applications, 2011, 38(3): 1482-1489.

[37] WANG H, SUN L L, VARADHARAJAN V. Purpose-based access control policies and conflicting analysis[C]//Security and Privacy-Silver Linings in the Cloud. Berlin: Springer, 2010: 217-228.

[38] WANG H, SUN L L, BERTINO E. Building access control policy model for privacy preserving and testing policy conflicting problems[J]. Journal of Computer and System Sciences, 2014, 80(8): 1493-1503.

[39] LI R H, JIANG Z J, WANG L F. Representing RCPBAC (role-involved conditional purpose-based access control) in ontology and SWRL[C]//International Conference on Brain Inspired Cognitive Systems. Berlin: Springer, 2018: 697-706.

[40] RIAHI S, KHOSRAVI R, GHASSEMI F. Purpose-based policy enforcement in actor-based systems[C]//Fundamentals of Software Engineering. Berlin: Springer, 2017: 196-211.

[41] AMINI M, OSANLOO F. Purpose-based privacy preserving access control for secure service provision and composition[J]. IEEE Transactions on Services Computing, 2019, 12(4): 604-620.

[42] BINTI ABDUL GHANI N, AHMAD M, MAHMOUD Z, et al. A pursuit of sustainable privacy protection in big data environment by an optimized clustered-purpose based algorithm[J]. Intelligent Automation & Soft Computing, 2020, 26(4): 1217-1231.

[43] WU G J, WANG S P, NING Z L, et al. Blockchain-enabled privacy-preserving access control for data publishing and sharing in the Internet of medical things[J]. IEEE Internet of Things Journal, 2022, 9(11): 8091-8104.

[44] LI F H, WANG W, MA J F, et al Action-based access control modelt[J]. Chinese Journal of Electronics, 2008, 17(3): 396-401.

[45] 李凤华, 王巍, 马建峰, 等. 协作信息系统的访问控制模型及其应用[J]. 通信学报, 2008, 29(9): 116-123.
LI F H, WANG W, MA J F, et al. Access control model and its application for collaborative information systems[J]. Journal on Communications, 2008, 29(9): 116-123.

[46] LI F H, WANG W, MA J F, et al. Action-based access control for web services[C]//Proceedings of the 2009 Fifth International Conference on Information Assurance and Security. Piscataway: IEEE Press, 2009: 637-642.

[47] 林果园, 贺珊, 黄皓, 等. 基于行为的云计算访问控制安全模型[J]. 通信学报, 2012, 33(3): 59-66.
LIN G Y, HE S, HUANG H, et al. Access control security model based on behavior in cloud computing environment[J]. Journal on Communications, 2012, 33(3): 59-66.

[48] 范艳芳, 韩臻, 曹香港, 等. 基于时间限制的多级安全模型[J]. 计算机研究与发展, 2010, 47(3): 508-514.
FAN Y F, HAN Z, CAO X G, et al. A multilevel security model based on time limit[J]. Journal of Computer Research and Development, 2010, 47(3): 508-514.

[49] 熊金波, 姚志强, 马建峰, 等. 基于行为的结构化文档多级访问控制[J]. 计算机研究与发展, 2013, 50(7): 1399-1408.
XIONG J B, YAO Z Q, MA J F, et al. Action-based multilevel access control for structured document[J]. Journal of Computer Research and Development, 2013, 50(7): 1399-1408.

[50] 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.
LI F H, WANG Y C, YIN L H, et al. Novel cyberspace-oriented access control model[J]. Journal on Communications, 2016, 37(5): 9-20.

[51] 谢绒娜, 郭云川, 李凤华, 等. 面向数据跨域流转的延伸访问控制机制[J]. 通信学报, 2019, 40(7): 67-76.
XIE R N, GUO Y C, LI F H, et al. Extended access control mechanism for cross-domain data exchange[J]. Journal on Communications, 2019, 40(7): 67-76.

[52] 李凤华, 孙哲, 牛犇, 等. 跨社交网络的隐私图片分享框架[J]. 通信学报, 2019, 40(7): 1-13.
LI F H, SUN Z, NIU B, et al. Privacy-preserving photo sharing framework cross different social network[J]. Journal on Communications, 2019, 40(7): 1-13.

[53] 谢绒娜, 范晓楠, 袁琳, 等. 在线社交网络中延伸访问控制机制研究[J]. 网络与信息安全学报, 2021, 7(5): 123-131.
XIE R N, FAN X N, YUAN L, et al. Research on extended access control mechanism in online social network[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 123-131.

[54] 张梦娇, 曹彦, 陶灵灵, 等. 在线社交网络中基于标签的访问控制研究[J]. 计算技术与自动化, 2018, 37(3): 141-145.
ZHANG M J, CAO Y, TAO L L, et al. Research on access control based on label in online social networks[J]. Computing Technology and Automation, 2018, 37(3): 141-145.

[55] 张涛. 数据标签在共享数据溯源中的应用研究[J]. 通信技术, 2020, 53(1): 221-224.
ZHANG T. Application of data labels in the traceability of shared data[J]. Communications Technology, 2020, 53(1): 221-224.

[56] KAPADIA A, AL-MUHTADI J, CAMPBELL R, et al. IRBAC 2000: secure interoperability using dynamic role translation[C]//Proceedings of the International Conference on Internet Computing. Berlin: Springer, 2003: 1-7.

[57] KHAMBHAMMETTU H, BOULARES S, ADI K, et al. A framework for risk assessment in access control systems[J]. Computers & Security, 2013, 39: 86-103.

[58] 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. New York: ACM Press, 2014: 293-304.

[59] OUTCHAKOUCHT A, ES-SAMAALI H, PHILIPPE J. Dynamic access control policy based on blockchain and machine learning for the Internet of Things[J]. International Journal of Advanced Computer Science and Applications, 2017, 8(7): 417-424.

[60] DI FRANCESCO MAESA D, MORI P, RICCI L. Blockchain based access control[C]//International Conference on Distributed Applications and Interoperable Systems. Berlin: Springer, 2017: 206-220

[61] 刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654.
LIU A D, DU X H, WANG N, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654.

[62] ZHANG Y, CHEN J, DU R Y, et al. FEACS: a flexible and efficient access control scheme for cloud computing[C]//Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. Piscataway: IEEE Press, 2014: 310-319.

[63] FISLER K, KRISHNAMURTHI S, MEYEROVICH L A, et al. Verification and change-impact analysis of access-control policies[C]//Proceedings of the 27th International Conference on Software Engineering. Piscataway: IEEE Press, 2005: 196-205.

[64] LI N H, TRIPUNITARA M V. Security analysis in role-based access control[J]. ACM Transactions on Information and System Security, 2006, 9(4): 391-420.

[65] 诸天逸, 李凤华, 金伟, 等. 互操作性与自治性平衡的跨域访问控制策略映射[J]. 通信学报, 2020, 41(9): 29-48.
ZHU T Y, LI F H, JIN W, et al. Cross-domain access control policy mapping mechanism for balancing interoperability and autonomy[J]. Journal on Communications, 2020, 41(9): 29-48.

[66] BERKAY C Z, TAN G, MCDANIEL P D. IoTGuard: dynamic enforcement of security and safety policy in commodity IoT[C]//Proceedings of the International Conference on Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2019: 23326..

[67] 张亚萍, 郭银章. 基于信任度与策略相似度的访问策略合成研究[J]. 计算机与数字工程, 2022, 50(3): 574-579.
ZHANG Y P, GUO Y Z. Research on access policy synthesis based on trust and policy similarity[J]. Computer & Digital Engineering, 2022, 50(3): 574-579.

[68] JOHANSEN H D, BIRRELL E, VAN RENESSE R, et al. Enforcing privacy policies with meta-code[C]//Proceedings of the 6th Asia-Pacific Workshop on Systems. New York: ACM Press, 2015: 1-7.

[69] BURKHALTER L, KÜCHLER N, VIAND A, et al. Zeph: cryptographic enforcement of end-to-end data privacy[J]. arXiv Preprint, arXiv: 2107.03726, 2021.

[70] ELNIKETY E, MEHTA A, VAHLDIEK-OBERWAGNER A, et al. Thoth: comprehensive policy compliance in data retrieval systems[C]//Proceedings of the 25th USENIX Security Symposium. Berkeley: USENIX Association, 2016: 637-654.

[71] WU Z P, WANG L F. An innovative simulation environment for cross-domain policy enforcement[J]. Simulation Modelling Practice and Theory, 2011, 19(7): 1558-1583.

[72] PEARSON S, CASASSA-MONT M. Sticky policies: an approach for managing privacy across multiple parties[J]. Computer, 2011, 44(9): 60-68.

[73] LENG C X, YU H Q, WANG J M, et al. Securing personal health records in the cloud by enforcing sticky policies[J]. TELKOMNIKA Indonesian Journal of Electrical Engineering, 2013, 11(4): 2200-2208.

[74] SPYRA G, BUCHANAN W J, EKONOMOU E. Sticky policies approach within cloud computing[J]. Computers & Security, 2017, 70: 366-375.

[75] KARJOTH G, SCHUNTER M, WAIDNER M. Platform for enterprise privacy practices: privacy-enabled management of customer data[C]//International Conference on Privacy Enhancing Technologies. Berlin: Springer, 2003: 69-84.

[76] 谢绒娜, 李晖, 史国振, 等. 基于区块链的可溯源访问控制机制[J]. 通信学报, 2020, 41(12): 82-93.
XIE R N, LI H, SHI G Z, et al. Blockchain-based access control mechanism for data traceability[J]. Journal on Communications, 2020, 41(12): 82-93.

[77] XIANG C C, WU Y D, SHEN B Y, et al. Towards continuous access control validation and forensics[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 113-129.

[78] ZYSKIND G, NATHAN O, PENTLAND A '. Decentralizing privacy: using blockchain to protect personal data[C]//Proceedings of the 2015 IEEE Security and Privacy Workshops. Piscataway: IEEE Press, 2015: 180-184.

[79] PINNO O J A, GREGIO A R A, BONA L C E D. ControlChain: blockchain as a central enabler for access control authorizations in the IoT[C]//Proceedings of the GLOBECOM 2017 - 2017 IEEE Global Communications Conference. Piscataway: IEEE Press, 2017: 1-6.

[80] CRUZ J P, KAJI Y, YANAI N. RBAC-SC: role-based access control using smart contract[J]. IEEE Access, 2018, 6: 12240-12251.

[81] MAESA D D F, MORI P, RICCI L. A blockchain based approach for the definition of auditable access control systems[J]. Computers & Security, 2019, 84: 93-119.

[82] PAILLISSE J, SUBIRA J, LOPEZ A, et al. Distributed access control with blockchain[C]//Proceedings of the IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2019: 1-6. [

[83] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management[C]//Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD). Piscataway: IEEE Press, 2016: 25-30.

[84] FERDOUS M S, MARGHERI A, PACI F, et al. Decentralised runtime monitoring for access control systems in cloud federations[C]//Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2017: 2632-2633.

[85] DENKER G, MILLEN J, MIYAKE Y. Cross-domain access control via PKI[C]//Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks. Piscataway: IEEE Press, 2002: 202-205.

[86] RAHMAN M U, GUIDI B, BAIARDI F. Blockchain-based access control management for decentralized online social networks[J]. Journal of Parallel and Distributed Computing, 2020, 144: 41-54.

[87] LYU Q Y, QI Y Z, ZHANG X C, et al. SBAC: a secure blockchain-based access control framework for information-centric networking[J]. Journal of Network and Computer Applications, 2020, 149: 102444.

[88] MANIATIS P, AKHAWE D, FALL K, et al. Do you know where your data are? secure data capsules for deployable data protection[C]//Proceedings of the 13th Workshop on Hot Topics in Operating Systems. Minnesota: University of Minnesota Press, 2023: 1-5.

[89] WANG L, NEAR J P, SOMANI N, et al. Data capsule: a new paradigm for automatic compliance with data privacy regulations[C]//Heterogeneous Data Management, Polystores, and Analytics for Healthcare.Berlin: Springer, 2019: 3-23.

[90] WANG L, KHAN U, NEAR J, ET AL. {PrivGuard}: privacy regulation compliance made easier[C]//Proceedings of the 31st USENIX Security Symposium.Berkeley: USENIX Association, 2022: 3753-3770.

[91] MEI H, HUANG G, CAO D G. Understanding “software definition” from the perspective of software researchers[J]. Communications of the CCF, 2015, 11(1): 68-72.

[92] HUANG G. Internet of Data: An infrastructure of digital space[J]. Communications of the CCF, 2021, 17(12): 60-62.

[93] 罗超然, 马郓, 景翔, 等. 数据空间基础设施的技术挑战及数联网解决方案[J]. 大数据, 2023, 9(2): 110-121.
LUO C R, MA Y, JING X, et al. Internet of data: a solution for dataspace infrastructure and its technical challenges[J]. Big Data Research, 2023, 9(2): 110-121.

[94] 张宁, 柳熠, 马新建, 等. 面向人机物融合的数联网标识解析技术[J]. 软件学报, 2024,35(10): 4681-4695.
ZHANG N, LIU Y, MA X J, et al. Identifier resolution technology for human-cyber-physical ternary based on Internet of data[J]. Journal of Software, 2024,35(10): 4681-4695.

[95] 窦悦, 易成岐, 黄倩倩, 等. 打造面向全国统一数据要素市场体系的国家数据要素流通共性基础设施平台: 构建国家“数联网”根服务体系的技术路径与若干思考[J]. 数据分析与知识发现, 2022, 6(1): 2-12.
DOU Y, YI C Q, HUANG Q Q, et al. Constructing a common data circulation infrastructure platform for the national unified data factor market: technical path and policy thinking of constructing the national “data networking” root service system[J]. Data Analysis and Knowledge Discovery, 2022, 6(1): 2-12.

[96] 李林, 任伏虎, 蔡华谦, 等. 基于时空码和数联网技术的新型“可信数据空间”体系构想[J]. 信息通信技术与政策, 2024(6): 89-96.
LI L, REN F H, CAI H Q, et al. Conception of new trusted data matrix system based on spatio-temporal coding and Internet of data technology[J]. Information and Communications Technology and Policy, 2024 (6): 89-96.

[97] International Data Spaces Association. Data spaces[R]. 2016.

[98] IEEE P3158 Trusted Data Matrix Working Group. IEEE P3158 standard for trusted data matrix system architecture[R]. 2024.

[99] 中国政府网. 可信数据空间发展行动计划(2024—2028年)[R]. 2024.
The Central People’s Government of the People's Republic of China. Action plan for the development of trusted dataspace[R]. 2024.

[100] KALOGEROPOULOS I, VLONTZOU M E, PSAROMANOLAKIS N, et al. EdgeDS: data spaces enabled multi-access edge computing[C]//Proceedings of the 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). Piscataway: IEEE Press, 2023: 424-429.

[101] TINON T A, ARNOLD F S, DENNIS M R. Designing for high availability a reference architecture for IoT data platforms[C]//Proceedings of the Pacific-Asia Conference on Information Systems. Piscataway: IEEE Press, 2024:1-17.

[102] HUTTERER A, KRUMAY B. The adoption of data spaces: drivers toward federated data sharing[C]//Proceedings of the 57th Hawaii International Conference on System Sciences. New York: ACM Press, 2024: 4506-4515.

[103] HUPPERZ M, GIEß A. The interplay of data-driven organizations and data spaces: unlocking capabilities for transforming organizations in the era of data spaces[C]//Proceedings of the 57th Hawaii International Conference on System Sciences. New York: ACM Press, 2024: 4496-4505.

[104] LOHMÖLLER J, PENNEKAMP J, MATZUTT R, et al. The unresolved need for dependable guarantees on security, sovereignty, and trust in data ecosystems[J]. Data & Knowledge Engineering, 2024, 151: 10-23.

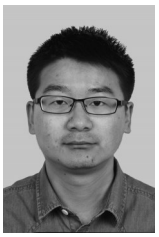
[105] GIEß A, HUPPERZ M, SCHOORMANN T, et al. What does it take to connect? unveiling characteristics of data space connectors[C]//Proceedings of the 57th Hawaii International Conference on System Sciences. Hawaii: ACM Press, 2024: 4238-4247.

[106] 陆志鹏. 安全可信数据空间的工程化路径研究[J]. 信息通信技术, 2023, 17(4): 49-55.
LU Z P. Research on the engineering path of secure and trusted data space[J]. Information and Communications Technologies, 2023, 17(4): 49-55.

[107] 陆志鹏. 数据要素流通体系的工程化研究[J]. 网络安全与数据治理, 2023, 42(4): 9-13.
LU Z P. Engineering research on data factor circulation system[J]. Cyber Security and Data Governance, 2023, 42(4): 9-13.

[108] 中国人大网. 人工智能与智能计算的发展[R]. 2024.
The National People’s Congress of the People’s Republic of China. The development of artificial intelligence and intelligent computing[R]. 2024.

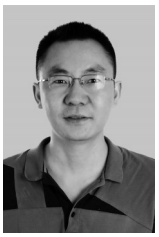
[作者简介]



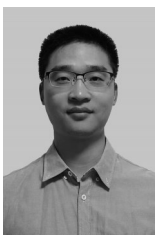
李恒（1990– ），男，陕西汉中人，中国科学院信息工程研究所博士生、高级工程师，主要研究方向为数据要素流通、访问控制、信息保护、隐私计算等。

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

史欣怡（1998– ），女，河南漯河人，中国科学院信息工程研究所博士生，主要研究方向为访问控制。



郭云川（1977– ），男，四川营山人，博士，中国科学院信息工程研究所正高级工程师、博士生导师，主要研究方向为访问控制。



郭守坤（1994– ），男，河南周口人，中国科学院信息工程研究所工程师，主要研究方向为隐私计算、数据安全。