计算机科学
COMPUTER SCIENCE

跨域数据管理

杜小勇, 李彤, 卢卫, 范举, 张峰, 柴云鹏

引用本文

杜小勇, 李彤, 卢卫, 范举, 张峰, 柴云鹏. 跨域数据管理[J]. 计算机科学, 2024, 51(1): 4-12.

DU Xiaoyong, LI Tong, LU Wei, FAN Ju, ZHANG Feng, CHAI Yunpeng. Cross-domain Data Management [J]. Computer Science, 2024, 51(1): 4-12.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.yg20240102

跨域数据管理

杜小勇　李　彤　卢　卫　范　举　张　峰　柴云鹏
数据工程与知识工程教育部重点实验室(中国人民大学)　北京 100872
中国人民大学信息学院　北京 100872

摘　要　随着数据成为新的生产要素和数字中国顶层战略的推进,跨域数据共享和流通对于实现数据要素价值最大化变得至关重要。国家通过布局全国一体化大数据中心体系、启动“东数西算”工程等一系列举措,为数据要素的跨域应用提供了基础设施。然而,传统的数据管理局限于单一域内,无法满足跨域场景下的数据管理需求。跨域数据管理面临通信层面的跨空间域挑战、数据建模层面的异构模型融合问题,以及数据访问层面的跨信任域挑战。从跨空间域、跨管辖域和跨信任域3个视角出发,探讨了跨域数据管理的内涵、研究挑战及关键技术,并展望了其未来发展趋势。

关键词:数据管理;跨空间域;跨管辖域;跨信任域
中图分类号　TP315

Cross-domain Data Management

DU Xiaoyong,LI Tong,LU Wei,FAN Ju,ZHANG Feng and CHAI Yunpeng
Key Laboratory of Data Engineering and Knowledge Engineering(Renmin University of China),Beijing 100872,China
School of Information,Renmin University of China,Beijing 100872,China

Abstract　As data becomes a new production factor and the digital China is promoted as a top-level strategy,cross-domain data sharing and circulation play a crucial role in maximizing the value of data factors. The country has taken a series of measures such as completing the overall layout design of the national integrated data center system and launching the “East-West Computing” project,providing infrastructure for the cross-domain application of data factors. Cross-domain data management faces challenges in communication,data modeling,and data access. This paper explores the connotation,research challenges,and key technologies of cross-domain data management from three perspectives:cross-spatial domain,cross-administrative domain,and cross-trust domain,and discusses its future development trends.

Keywords　Data management,Cross-spatial domain,Cross-administrative domain,Cross-trust domain

1　引言

数据是新的生产要素,数字中国是国家的顶层战略,对实现中国式现代化将发挥重要作用。为此,国家正在大力发展各种数据基础设施。2022年初,我国完成了全国一体化大数据中心体系的总体布局设计,并正式启动了“东数西算”工程。该工程在京津冀、长三角、粤港澳等八大区域设立了国家枢纽节点,旨在构建全国一体化的算力网络。“东数西算”工程为数据要素在数字世界中的跨域共享和流通提供了关键基础设施。2022年底,国家又出台了数据要素基础制度(简称“数据二十条”),成立了国家数据局,其任务之一就是要进一步落实数据要素的基础制度。可以设想,数据要素将在我国的经济社会生活中发挥越来越大的作用。

数据要素的价值遵循著名的梅特卡夫法则:参与数据共享和流通的市场主体数目越多,数据的价值越大,“增值”就以指数级变大。为了实现数据要素价值的最大化,实现数据要素的跨域共享和流通成为了必然。例如,市场主体可以汇聚汇通多种业务系统的数据,孕育新的实体业务或数据价值业务,从而使数据要素产生更大的价值。

跨域数据共享和流通,需要在跨域场景下进行数据管理。数据管理指利用计算机技术对数据进行高效、安全、经济的采集、加工、存储和运用的过程。简单来说,数据管理是一种技术,旨在确保数据在不同时间节点上始终保持正确性、一致性、可用性和安全性。然而,传统的数据管理通常仅限于单一企业、业务或数据中心内部,尽管有些分布式数据管理系统采用了多地备份的方案,但其主要用于应对灾难等特殊情况。面对日益增长的跨域数据共享和流通需求,需要升级现有数据管理技术,确保数据要素价值在跨域场景下有序、高效、安全地共享和流通。

跨域数据管理,是数据管理从面向和限定于单域的孤立服务发展到跨域的共享与协同服务阶段的产物。跨域为数据管理带来了全新的挑战:通信层面,数据管理面临跨空间域的挑战,体现为不确定性网络的问题;数据建模层面,数据管理面临多模型和多模式的挑战,体现为异构模型融合的问题;

到稿日期:2023-11-20　返修日期:2023-12-22
通信作者:杜小勇(duyong@ruc.edu.cn)

数据访问层面，数据管理面临跨信任域的数据访问、数据价值发现和快速构建业务系统的挑战。本文从跨空间域、跨管辖域和跨信任域3个视角，阐述跨域数据管理的内涵、研究挑战及对应的关键技术，并探讨未来的发展趋势。

2 跨域数据管理的内涵

传统数据管理的边界在于数据的存储和组织（如数据模型和数据索引）、查询和优化、事务管理（如并发控制和故障恢复）等方面，其服务对象通常为单一组织。评估传统数据库的主要指标包括高可用性、高性能和高安全性。随着云计算的发展，云数据库系统逐渐崭露头角，其主要特点为功能分离，尤其是存算分离，且逐渐扩大到其他功能的分离，如事务管理器、查询优化器等。

在数字中国的背景下，数据管理应将发挥数据要素的价值作为其追求的主要目标之一。因此，数据管理的边界需要扩展，应包括数据的汇聚融合、可信流通和价值挖掘等功能。此外，还需要考虑数据要素分布在不同数据中心的场景以及数据安全和隐私保护问题。这些都是被传统数据管理所忽略或重视不足的方面，我们将其统称为跨域数据管理。

相比传统数据管理，跨域数据管理呈现出以下3个新的特征：

1）跨空间。数据和系统部署经常跨越城市和国家，分布距离达到100 km以上，甚至上千、上万公里。光速的限制导致传输延迟至少达到毫秒级别，与数据中心内部微秒级通信延迟相差几个数量级，即不能通过计算机软硬件技术的作用，将访问延迟隐藏起来，需要针对这一瓶颈对系统进行重新设计和构造。

2）跨管辖。跨域业务涉及多个系统，跨域部门、系统之间通常数据标准不同、数据模型不同、访问控制机制不同，甚至对数据安全和数据隐私保护的要求也不同，因此必须解决跨管辖域的问题，让不同管辖域的数据能够互相对齐，相互操作，统一查询。

3）跨信任。跨域部门、系统之间互相不信任，不希望完全公开和共享自己的私有数据。这种情况下，一般很难进行统一的增删改操作，但是跨域业务往往需要实现统一的数据查询，关联更多私域数据，可以挖掘出更大的数据价值。

根据上述特征，跨域数据管理可以细分为跨空间域数据管理、跨管辖域数据管理和跨信任域数据管理[1]。值得一提的是，如图1所示，由于跨空间域、跨管辖域和跨信任域是看待跨域数据管理的3个不同的视角，并不是正交的划分，因此研究内容存在交叉在所难免。下文分别从跨空间域、跨管辖域和跨信任域3个视角来对跨域数据管理的内涵进行解读。

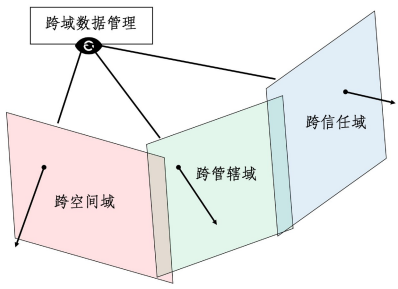

图1 跨域数据管理的3个视角

Fig. 1 Three perspectives on cross-domain data management

1）跨空间域视角，主要解决高时延、高波动广域网所带来的数据管理性能优化问题。需要研究高性能高可靠的数据同步等跨空间域数据存储技术，查询算子下推到存储节点等近数计算优化等跨空间域数据查询优化技术，以及跨空间域事务处理和数据传输等优化技术等。

2）跨管辖域视角，主要解决不同主体之间数据要素共享和协同问题。需要研究不同模型、不同模态、不同语义、不同标准之间的异构数据汇聚与融合关键技术，包括统一表达与查询关键技术等。

3）跨信任域视角，主要解决不同域间数据要素可信流通以及价值利用中涉及的安全、完整性、合规性、可信以及个人隐私保护等一系列问题。需要研究保护数据隐私安全的访问控制机制、审计跟踪、可信硬件等技术，保障数据机密性的数据加密、数据脱敏以及安全计算等技术，建立综合的防篡改数据管理框架，包括但不限于区块链技术、数据标准化与元数据管理，以及身份验证与授权管理等。

3 跨空间域数据管理技术

跨空间域数据管理技术的研究与传统的数据管理技术的研究类似，但跨空间域带来的性能和可用性方面的挑战尤为突出。因此，本章主要从跨空间域的分布式数据库系统性能和可用性方面，针对跨空间域数据存储、跨空间域数据查询和跨空间域事务处理这3个问题进行讨论。

3.1 跨空间域数据存储

跨空间域数据存储主要通过分布式一致性共识协议（如Paxos/Multi-Paxos[2]，ZAB[3]，Raft[4]等），实现副本间的日志同步。一致性共识协议包含两个核心模块：领导者选举（Leader Election）和日志复制（Log Replication）。领导者（Leader）是系统中的一个特殊节点，当某个节点获得大多数节点的投票时即可当选领导者。领导者负责与客户端通信，并协调其他跟随者（Follower）节点上数据副本的复制与同步。日志复制指系统中的节点接收到数据后会将数据副本复制到一个或多个其他节点。日志复制的基本功能是实现数据备份，提升系统可用性。一致性共识协议副本间的日志同步能力，是数据库高可用能力的核心竞争力，是金融核心系统、有云业务等场景的关键痛点。然而，广域网的网络时延绝对值增大、网络时延差异性不可忽略和网络时延动态变化，使得跨空间域分布式数据库的日志同步成为影响系统性能的瓶颈，给跨空间域数据管理带来了巨大的挑战。针对传统的一致性共识算法在单一数据中心内运行良好，但在跨数据中心之间运行不佳的难题，近年来，业界提出了一些可能适用于跨空间域场景的一致性共识协议的初步改进方案，希望更好地满足跨空间域数据管理的需求。

在领导者选举方面，基本的优化思路是通过提高日志同步的通信效率，来提升系统性能。Xu等[5]提出了网络时延感知的领导者选举算法Raft-Plus，其核心思想是在Raft的基础上，将节点之间的网络时延作为领导者选举的依据，通过选取时延最优的节点作为领导者来提升系统性能。同时Raft-Plus引入了一种反对票机制，当跟随者发现其与领导者的网络时延超出阈值时，则向领导者发送反对票；当领导者收到一半

以上的反对票时则将领导者角色切换为跟随者。Sakic 等[6]提出的 SEER 不仅考虑了节点之间的网络时延，还考虑了副本的资源利用率和可用性等因素，对 Raft 协议的领导者选举算法进行优化。上述工作属于针对单一领导者(Single-Leader)系统的优化。近年来，多领导者(Multi-Leader)系统由于可以更好地支持跨空间域数据管理中的就近读写需求，受到了越来越多的关注。例如，Vukolic 等[7]提出了多领导者集合筛选方案 Droopy/Dripple，基于历史工作负载和系统响应延迟，策略性地配置其领导者集合，从而减少了系统在工作负载不平衡情况下的响应延迟。

在日志复制方面，基本的优化思路是通过降低日志同步的通信需求来提升系统性能。例如，Park 等[8]提出 CURP，在领导者和跟随者的基础上，通过新角色见证者(Witnesses)，客户端将每个操作请求复制给一或多个见证者，同时向领导者发送请求。领导者执行操作并返回客户端，无需等待数据复制到其他跟随者，其允许数据操作在一轮通信内完成，通过减少日志复制过程中的通信次数，从而提升系统性能。与 CURP 不同，EPaxos[9]是一种无领导者(Leader-Less)的分布式共识算法。所有副本都可以从客户端接受请求，只需一轮通信即可提交请求。若要降低通信需求，除了减少通信次数外，还可以像 DPaxos[10]一样，通过将用户所需数据分片分配到距离用户请求发出位置最近的数据中心，从而降低跨空间域的日志同步时延。

尽管上述方案为解决跨空间域一致性共识协议设计提供了思路，但它们仍存在一些局限。例如，Raft-Plus 等对 Raft 的领导者选举的优化未经具体分析和方案论证；CURP 和 EPaxos 依赖于操作的交换性假设，适应的场景受限；DPaxos 主要适用于边缘计算系统，同样缺乏通用性。总体而言，跨空间域数据存储技术仍处于起步阶段，还需要在通用性、有效性、可靠性等核心问题上进行深入研究。

3.2 跨空间域数据查询

跨空间域数据查询优化技术的目标是在数据库查询优化引擎生成一个执行策略的过程中，尽量使查询的总开销(包括 I/O、CPU、网络传输等)达到最小。跨空间域数据查询优化除了考虑 CPU 代价和 I/O 代价外，还要考虑通过节点间传输数据的代价，要尽量减少查询过程中的数据传输的次数和数据量，从而减少因网络通信瓶颈带来的查询性能下降的负面影响。

近年来，业界提出了一些可适用于跨空间域场景的查询策略优化方案。例如，Pu 等[11]提出了 Iridium，通过基于贪婪的方法优化数据和任务的编排，避免了数据聚合到同一数据中心导致的查询响应时延大的问题；Obasi 等[12]基于图形数据库在管理多个关系方面效率高的特性，使用改进的 GraphQL 模型和随机森林算法来提高分布式数据库中的查询性能；Dong 等[13]提出使用统一接入层和可扩展查询引擎，可以监控查询性能并生成替代查询执行计划或策略，从而提高混合多云数据库环境中的查询性能；Lu 等[14]提出通过引入索引、缓存、过滤、Map-Reduce、查询执行计划、数据分区等技术来提高分布式大数据系统中的查询性能；Dong 等[15]结合了蚁群算法的全局优化能力和模拟退火算法的局部优化能力，以加快分布式数据库的检索速度；Lin 等[16]讨论了一种通过分布式查询引擎并将表数据拆分成碎片块进行并行计算来提高分布式数据库中查询性能的方法。上述方案为跨域分布式数据库查询策略优化提供了思路，但是大部分方案都存在一个问题，即依赖在线启发式方法来进行最优策略的决策，无法保证总是能得出最佳解决方案。同时，这些方案在大规模部署或高负载网络场景中的可扩展性和性能还有待进一步地深入研究。

3.3 跨空间域事务处理

跨空间域事务处理技术主要关注如何面向不确定性网络进行高效的分布式事务调度和编排。事务是用户定义的一组数据库操作组成的序列，是数据库管理系统中的最小执行单元。分布式事务指在事务中包含对不同节点上的数据项的操作，当服务端收到一个分布式事务时，通常将其交由一个协调者来负责。在执行阶段，协调者将事务拆分成多个子事务并分发给各个参与者，参与者根据并发控制算法执行事务，例如，如果采用两阶段封锁协议(Two-Phase Lock，2PL)作为并发控制协议，参与者将在执行阶段对数据项进行加锁，这适用于高冲突场景，但会降低系统的并发度并且需要考虑死锁问题；如果采用乐观并发控制协议(Optimistic Concurrency Control，OCC)，参与者在执行阶段不需要对数据项加锁，也不需要在提交前对数据项进行验证，这适用于低冲突场景。在执行阶段结束后，分布式数据库通常采用两阶段提交协议(Two-Phase Commit，2PC)来保证数据库的一致性。2PC 将事务提交分成了两个阶段。在准备阶段，协调者收集各参与者的执行状态，并根据各子事务的执行结果确定事务的最终状态。如果所有参与者都可以提交事务，那么协调者将事务状态设置为“提交”(Commit)并通知各参与者；否则，任何一个参与者无法提交，协调者都会将事务状态设置为“回滚”(Rollback)，同时通知所有的参与者将子事务回滚。

近年来，“两地三中心”“三地五中心”等概念被提出，这意味着数据库将会处理越来越多的跨空间域分布式事务。分布式事务处理需要两阶段提交协议来保证各参与节点子事务提交的原子性。在跨空间域场景下，节点之间的网络时延更长且存在差异性，传统的事务处理技术需要拓展，以保证系统能够提供较高的吞吐量。近年来，业界提出了一些针对跨空间域场景的分布式事务处理的初步改进方案，希望能够更好地满足跨空间域数据管理的需求。例如，Zhang 等[17]提出的 RedT 结合了准备阶段，通过在执行阶段减少数据通信次数，并在执行阶段写入重做日志以消除日志准备阶段的同步，提高事务处理吞吐量并降低事务处理延迟；Yan 等[18]和 Mu 等[19]则采用将 2PC 协议与共识协议相结合的方式，减少了事务提交所需的数据通信次数。其他工作如 GPAC[20]和 TAPIR[21]也试图将事务提交阶段和共识协议有机融合，通过在 2PC 阶段并行执行日志复制，以减少日志复制过程中的通信次数。另一方面，Ren 等[22]提出的 SLOG 方法通过将事务分为单归属事务和多归属事务两类，进一步优化了跨域数据库

的性能。对于数据所在区域与事务发起区域相近的单归属事务，SLOG 选择就近发起事务，避免了全局协调的开销。对于多归属事务和从主副本物理距离较远的地方发起的单归属事务，SLOG 采用动态数据重选主的策略，根据特定位置的访问频率随时间变化进行选择，解决了最具挑战性的多归属事务执行问题。即使在大量多归属事务存在数据访问争用和需要跨物理距离的区域进行协调的情况下，SLOG 也能保持严格的串行化和高吞吐量。

这些方法虽然为跨空间域事务处理的后续研究提供了有益的参考，但也存在相应的局限性。例如，上述算法均是在读/写集已知的假设下设计的，而这一假设在大多数跨域数据管理场景中都难以满足。另外，这些方案都需要对数据库内核进行侵入式修改，存在部署层面的挑战。

4 跨管辖域数据管理技术

传统的数据管理主要局限于单一企业、业务、数据中心等单管辖域场景，研究的重点是如何利用数据库等技术，高效地对数据进行获取、存储、处理和使用。然而，数据高效共享流通的巨大需求正迫使数据管理从面向和限定于单管辖域的孤立服务发展到跨管辖域的共享与协同服务的阶段，也直接催生了跨管辖域数据管理的巨大需求。图 2 给出了在城市治理场景下跨管辖域数据管理的一个示意图，数据具有跨管辖域特性，即分散在不同的部门、层级和主体。同时，应用场景如城市运行、公共服务等的问题也很难使用单一领域的数据来解决，因此需要为数据跨管辖域高效共享流通提供理论与技术支撑。

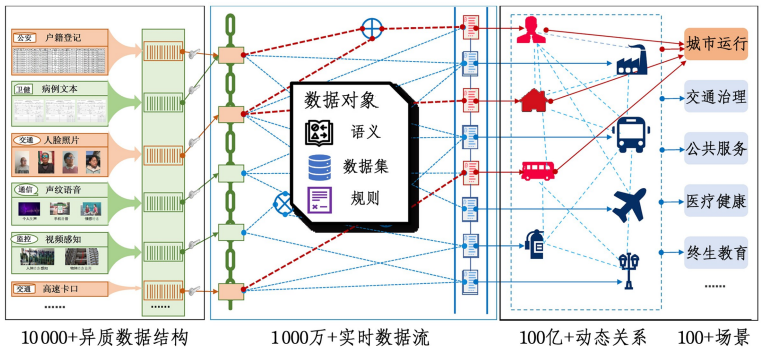

图 2 跨管辖域数据管理：以城市治理场景为例[23]

Fig. 2 Cross-jurisdictional data management: take the urban governance scenario as an example[23]

与以数据库为代表的传统数据管理技术相比，跨管辖域数据管理面临的挑战突出体现在以下 3 个层面：

1）跨管辖域数据异质语义与统一语义表示之间的矛盾。数据管理跨多个管辖域，在数据语义层面呈现出显著的“跨域异质”的特点，主要体现在以下两个方面：(1)同名不同义，例如“单位”在城市管理委是“法人单位”的含义，而在交通委是“监测数据单位”的含义；(2)同义不同名，例如“身份证件号码”在不同部门办事过程中的名称有所不同，如“公民身份证号”“证件号码”等。因此，为了更好地支持数据高效共享，跨管辖域数据管理迫切需要进行高质量语义融合，为异质数据提供统一的语义表示。

2）跨管辖域数据多模存储与高效查询处理之间的矛盾。数据管理跨多个管辖域，在数据存储层面呈现出显著的“跨域多模”的特点，这里的“多模”包含两层含义：(1)不同管辖域具有独立的数据模型，如关系数据模型、图数据模型等；(2)不同管辖域具有不同的数据模态，如表格、文本、流、图像、声音等。因此，为了更好地支持数据高效共享，跨管辖域数据管理需要设计高效的查询处理机制，提升数据查询的性能。

3）跨管辖域数据多样规则与可信访问控制之间的矛盾。数据管理跨多个管辖域，在数据访问层面呈现出显著的“规则多样”的特点。这里以公民车辆信息为例，该信息在不同的管辖域允许暴露的内容有明显的分级特点，例如在某些管辖域只允许暴露“有无”车辆内容，在某些管辖域可以暴露具体的车辆数量，而在另外一些管辖域可以进一步暴露车辆详情。同时，不同的管辖域允许其他管辖域在其数据上执行的操作也不尽相同，如筛选、分组、聚合等。为了更好地支持数据高效共享，跨管辖域数据管理需要设计统一的数据访问控制机制，保证数据在不同管辖域之间能够可信地进行共享流通。

本章主要探讨解决上述 3 方面问题的关键技术，主要包含：跨域数据融合语义表示、跨域数据融合查询处理、跨域数据融合访问控制。下面具体介绍现有的解决方案、尚未解决的难题与未来的发展趋势。

4.1 跨域数据融合语义表示

跨域数据融合语义表示，也称数据融合(Data Curation)，其目标是整合多源异质数据，提升整体数据质量，最终形成统一且高质量的数据视图，包括模式匹配、实体对齐、冲突消解、缺失值填充、异常值检测等种类繁多的任务。由于大数据在规模与多样性方面面临挑战，跨域数据融合语义表示费时费力，并已成为大数据由价值向赋能转化的主要瓶颈。

图灵奖获得者 Michael Stonebraker 教授将数据融合的发展历程归纳为三代[24]。第一代是面向数据仓库等应用场景的抽取-转换-载入(ETL)工具，主要解决小规模数据源的融合问题。第二代是面向大规模数据源融合中的异质性挑战，利用深度学习等技术解决面向领域的融合问题。近年来，研究者也针对特定领域不同种类的融合任务，设计了基于小型语言模型的数据融合清洗方法，包括语义标注、缺失值填充、实体链接、实体匹配、实体对齐。国内学者的研究也在相关领域取得了一定进展。中国人民大学范举等在将小型语言模型

应用于数据融合方面做了系列工作，包括数据清洗[25]、数据匹配[26-27]等。浙江大学的高云君等研究了小型语言模型提示学习算法在实体匹配问题上的效果[28]。这些工作初步验证了小型语言模型解决此类问题的可行性。第三代是研究跨领域通用的数据融合系统，但这方面的研究还处于探索阶段。香港大学和卡耐基梅隆大学的研究者提出了多任务小样本学习的方法，通过设计统一的框架来完成结构化知识相关的数据融合任务[29]。中国人民大学的研究者提出了一个通用编码器融合异质数据，混合多种专家模型增强数据表示，设计了多任务数据匹配模型[26]。

总体来看，现有的工作主要解决面向领域的数据融合问题，即面向特定任务、特定领域或特定数据集设计数据融合的方法与工具。尽管近年来出现了一些基于预训练语言模型的数据融合研究，但这些研究主要是利用参数规模有限的小型语言模型，亟需系统地研究如何利用参数规模更大的大模型构建通用的数据融合系统。

4.2 跨域数据融合查询处理

查询处理与优化是数据管理最核心的功能之一。跨管辖域数据查询面临着两个关键挑战：1）缺乏统一的查询语言。不同数据管理域的数据库具有独立的数据模型和查询语言，如关系数据模型与 SQL 语言、图数据模型与 Cypher 语言等。由于不同域数据库所蕴含的数据模型和查询语言彼此不通，因此无法直接进行统一的查询。2）缺乏统一的优化机制。查询优化对于数据管理来讲至关重要，同一查询的不同优化结果可能会有数量级的性能差异。然而，不同数据模型的数据库适用的场景各异。例如：图数据库适合路径查询、模式匹配查询等；关系数据库适合选择查询、聚集、统计、连接查询等；向量数据库适合矩阵运算等。结合上层应用的特点，研究统一的查询优化方法对于提升整体查询性能非常关键，也颇具挑战性。

上述挑战给现有的数据管理技术带来了新的难题，主要的解决方案有以下 3 类：物理汇聚、联邦数据库（Federate Database）以及多存储数据库（Polystore Database）。物理汇聚利用抽取-转换-载入（Extract-Transform-Load，ETL）技术，将数据物理汇聚到同一个数据库进行统一管理。联邦数据库将多个自治的同构数据库模式映射到一个全局视图中，进而基于该全局视图进行统一查询与优化。不难看出，上述两类方法并不适用于跨域数据管理的场景，因而近年来多存储数据库系统受到了学术界和工业界的广泛关注。下面仅对多存储数据库系统进行介绍。

针对统一数据模型的挑战，多存储数据库系统的研究可以分为松耦合、紧耦合以及混合系统。松耦合多存储系统，如 BigIntegrator[30]，Forward[31]等，采用中介器-包装器架构。紧耦合多存储系统，如 Polybase[32]，HadoopDB[33]等，可以在查询执行期间直接访问底层数据库，并使数据在不同数据库之间进行高效移动。混合系统结合了松耦合系统与紧耦合系统的优点，代表性的研究包括 Spark SQL[34]，BigDAWG[35]等。针对语义融合挑战，学者们研究了数据融合技术，目标是整合多源数据的异构语义，形成统一的数据视图。谷歌公司推出了 Cloud Dataprep[36]，利用 Trifacta 数据准备工具[37]与用户进行交互，推荐和预测数据融合操作，缩短用户数据融合的时间。图灵奖获得者 Michael Stonebraker 教授主导开发了 Tamr 系统[38]，重点解决多源数据融合场景中的语义融合难与数据质量低等问题。

总的来说，现有工作尚未针对跨域异构数据存在的模型各异、松散耦合、彼此自治等挑战设计通用的方法与高效的系统，更多地是解决一些具体的技术与算法问题。此外，现有方法更侧重于关注多模型（Multi-Model）数据，而非多模态（Multi-Modal）数据。如何面向关系、文本、图、流等多模态数据，提供高性能的查询处理，是一个亟待研究和突破的难题。

4.3 跨域数据融合访问控制

跨管辖域数据管理需要提供一个面向多方数据协作的访问控制机制，该机制应允许数据在两个或多个不同的主体（不同部门、不同层级、不同国家）之间共享使用的同时，在全生命周期满足不同管辖域访问控制规则的要求。由于不同管辖域在数据访问控制规则方面具有多样性，因此，提供一个融合的访问控制方法至关重要。

学术界和工业界均对该领域展开了研究。美国伯克利大学的学者提出了“数据胶囊”的概念[39]，并基于这一概念开发了 PrivGuard 系统[40]。数据胶囊的基本想法是对数据访问控制的合规性进行自动检查，并将这一检查过程与数据管理的整个生命周期相关联（如数据转换、数据聚合、数据查询等）。在工业界，美国的亚马逊和 Snowflake 等企业纷纷推出了数据净化室（Data Clean Rooms）项目；在国内，蚂蚁公司推出了隐语项目。这些项目的核心都是提供一个统一的平台，在支撑各方进行数据共享使用的同时，保证数据的访问控制满足不同管辖域的多样化规则要求。

综上，现有工作更多的是面向具体的应用开发融合的跨管辖域数据融合访问控制方法，解决了一些具体的策略与算法问题，并没有开发出通用的跨域数据融合访问控制系统。这是一个亟待解决的难题。

5 跨信任域数据管理技术

信任域是一种数据管理安全控制机制，是由各个企业、组织或机构所设置的本地认证服务所组成的相对独立的域[41]。每个信任域中都包含着不同的用户、网络资产和数据对象，这些都是用来控制访问权限的主要手段[42-44]。然而，信任域的存在，也会造成在数据管理过程中产生分散的“数据孤岛”问题[45]，这会阻碍机构之间进行数据共享和协同工作。因此，我们需要寻找一种更加高效的数据管理解决方案，来打破这些数据孤岛，促进机构之间的合作和信息共享。

5.1 数据隐私保护

在跨信任域数据管理领域，数据隐私保护问题至关重要[46]。数据隐私保护指在数据处理和传输过程中，采取各种措施来保护数据的机密性、完整性和可用性，防止数据被未经授权地访问、修改、删除，从而避免信息泄露[47-48]。数据隐私保护涵盖了访问控制、审计跟踪、差分隐私、数据生成、数据脱敏等技术手段。在跨信任域数据管理中，不同的企业、组织或

机构通过设置本地认证服务形成了相对独立的信任域,这些信任域之间的数据共享和工作协同迫切需要有效的隐私保护措施来保障数据的安全性。

访问控制是实现既定安全策略的系统安全技术,它负责管理所有资源的访问请求,并根据预先设定的安全策略做出授权决策,有效地防止合法用户进行非法资源利用[49]。审计跟踪技术则是针对监测和记录系统或网络中发生的各种事件、活动和操作的技术,其目的在于帮助管理者识别潜在的威胁或安全漏洞,从而采取相应的措施来应对或预防可能出现的安全问题[50]。此外,跨信任域数据管理还可以采用数据脱敏和匿名化技术来保护数据的隐私[51],使得数据仅能够被授权的信任域及人员访问和使用。同时,作为隐私保护技术的基础,建立全面的数据管理和共享框架对于跨信任域数据管理至关重要。例如,可以制定数据共享协议和数据访问控制策略,明确数据的使用规则和权限控制机制,以确保数据的安全和合规性[52]。

总之,数据隐私保护和跨信任域数据管理是密不可分的,只有采用合适的技术手段和建立完善的数据管理机制,才能够确保数据的安全性和进行隐私保护,促进跨信任域数据的共享和协同工作,为企业和组织的发展提供支持和保障。

5.2 数据加密

跨信任域数据管理需要在不同的信任域之间进行数据共享和协同工作。为了防止数据在流通过程中泄漏,数据加密成为了跨信任域数据管理的关键技术手段。数据加密是一种通过算法将原始数据转换为密文的技术[53-54]。在数据加密过程中,原始数据会经过特定的加密算法处理,生成一串看似随机的密文。只有持有正确密钥的信任域人员才能解密并将其还原为可读的原始数据,从而保护了数据的机密性,防止出现未经授权的访问和窃取[55]。同态加密技术则支持数据在加密状态下进行计算,无需解密数据[56]。数据加密是跨信任域中的重要技术手段,被广泛应用于各类信息系统和网络通信中,以保护敏感数据的安全[57-60]。

数据加密技术与跨信任域数据管理之间存在着密切的联系。首先,数据加密技术可以在数据传输和存储过程中保护数据的机密性,防止数据在跨信任域传输或存储时被未经授权地访问。对数据进行加密后,即使数据在跨信任域传输或存储过程中被截获,也无法被解读和利用,从而保护了数据的安全。其次,数据加密技术也可以在跨信任域数据共享和协同工作中起到重要作用。在跨信任域数据管理中,不同的信任域可能具有异构的存储计算资源和不匹配的安全策略以及访问权限控制机制,因此需要对数据本身采取措施来保障安全性。加密技术允许安全地共享数据而无须担心信任域之间的安全差异。即使在不同的安全环境中,只要有正确的解密密钥,数据就可以被正确地解密和访问。此外,数据加密技术还可以与访问控制和身份认证等安全技术结合,构建起完善的跨信任域数据管理系统,以确保数据的安全性和合规性。通过对数据进行加密,并结合访问控制和身份认证技术,可以实现对数据访问权限的精细控制,确保数据只能被授权的用户访问和使用。

总之,数据加密是跨信任域数据管理中不可或缺的技术手段。采用数据加密技术,可以在跨信任域数据管理中保护数据的安全和隐私,促进数据的安全共享和协同工作,为企业和组织的发展提供支持和保障。

5.3 数据防篡改

在跨信任域数据管理中,数据防篡改也是非常重要的问题。数据防篡改指通过各种技术手段,保护数据在传输、存储和处理过程中不被未经授权人员篡改、修改或损坏的安全措施[61]。在跨信任域数据管理中,数据防篡改技术旨在确保数据的完整性和可信度,防止数据被篡改后对任一相关信任域的业务和决策产生不良影响。例如,区块链技术是一种分布式数据库技术,它以区块的方式存储数据,并使用密码学技术确保数据的安全性和完整性,可以保证跨域数据管理中数据不会被篡改[62-63]。区块链技术最初是作为比特币的底层技术而出现的,但现在已经被广泛应用于金融、供应链管理、医疗保健、物联网等领域[64]。

数据防篡改技术与跨信任域数据管理之间存在着密切的联系。首先,数据防篡改技术可以在数据传输和存储过程中保护数据的完整性。采用数据防篡改技术,可以对数据进行数字签名和校验,确保数据在跨信任域传输和共享过程中不会被篡改或损坏,同时也能够满足不同信任域的安全要求[65]。其次,采用数字签名、哈希算法等技术手段,数据防篡改技术也可以在跨信任域数据共享和协同工作中起到维持数据可信性和修改可追溯性的重要作用[66]。在跨信任域数据管理中,防篡改技术在数据进入信任域前对数据完整性进行检测,通过警告或拒绝使用篡改数据、记录事件、恢复原始数据或触发安全机制等方式,确保信任域内数据的安全性。此外,数据防篡改技术与访问控制、身份认证、数据加密等安全技术结合,可构建起完善的跨信任域数据管理系统,提供多层次的保障[67]。通过对数据进行数字签名和校验,结合访问控制和身份认证技术,可以实现对数据传输和共享过程的安全监控和控制,确保数据的安全、完整和可信。

总之,数据防篡改技术与跨信任域数据管理技术之间存在着密切的联系。采用数据防篡改技术,可以在跨信任域数据管理中保护数据的完整性和可信度,促进数据的安全共享和协同工作,为企业和组织的发展提供支持和保障。

结束语 本文从跨空间域、跨管辖域和跨信任域3个视角出发,对跨域数据管理的内涵和关键技术进行了解读和讨论。需要承认,到目前为止,跨域数据管理的相关研究还处于初级阶段,相应的技术体系还不成熟。为了进一步完善跨域数据管理的技术框架,未来的研究需要重点关注以下几个方面。

1)跨空间域数据管理方面,可以围绕如何解决跨域带来的网络通信瓶颈问题来展开。具体地,通信瓶颈有以下3种解决思路:(1)降低通信需求。通信需求指通信的次数和数据量。跨空间域数据管理系统中的分布式节点之间交互数据量越大或者通信越频繁,跨空间域数据管理业务中网络通信开销就越大,通信瓶颈的负面影响也越大。因此,未来可以在分布式共识协议、查询策略、事务处理等方面,基于多主(Multi-

Master)架构、数据布局(Placement)优化和就近计算等思想,降低通信需求。(2)提高通信效率。在通信需求一定的情况下,提高通信效率可以提升跨空间域数据管理系统的性能。例如,通过选择网络条件最好的节点作为领导者节点,可以提高节点之间通信效率,从而提升分布式数据库系统的日志同步性能;通过对每个节点设置不同的心跳间隔,使节点能够尽早发送日志数据,也可以提升系统性能;根据网络时延的差异性,延迟部分子事务的执行,通过减少事务锁争用时长,可以提高锁资源的利用率,从而提升事务并发处理性能。(3)提升通信能力。通信能力的提升需要进一步深入研究广域确定性网络技术。一方面,改良式路线的确定网络技术,可以基于跨层思想、多路径和 AI 等技术手段进行持续演进[68];另一方面,革命式路线的确定性网络技术,需要进一步推动确定性广域网基础设施建设和革命式路线技术的标准化[69]。同时,从确定性服务质量(QoS)到确定性业务体验(Quality of Experience,QoE),也是未来重要的研究方向。

2)跨管辖域数据管理方面,可以围绕高质量数据融合展开,主要解决以下几个难点:(1)跨域数据通常采用不同的模型来描述数据,因此会带来数据模型不统一的挑战;(2)跨域数据往往存在"一数多义""一义多数"等语义难题,因此会带来数据语义难对齐的挑战;(3)数据融合的结果质量与融合成本通常此消彼长,难以兼顾,因此会带来质量成本难优化的挑战。针对这些挑战,研究面向数据要素共享流通的统一数据模型抽象,支持数据跨域访问的数据模型融合;研究语义异构性等难题,实现异构数据的语义融合;建模融合质量与成本之间的相关性,设计通用的质量成本优化算法。

3)跨信任域数据管理方面,可以针对分散的"数据孤岛"之间的数据共享与协同展开,主要解决如下难题:(1)跨信任域数据存储和使用过程中,如何通过数据隐私保护来保证数据的机密性、完整性和可用性;(2)跨信任域数据传输过程中可能存在数据泄漏,传统加密技术也存在资源开销大等问题;(3)在跨信任域数据传输、存储和管理的过程中,保证数据不被篡改也是跨信任域数据管理面临的挑战。围绕这些挑战,可以研究面向数据要素在不同信任域数据库系统异构、存储模式异构的汇聚和共享;研究数据加密过程中软硬件性能、资源开销瓶颈;构建基于高效区块链去中心化和留痕不可篡改的多信任域数据库系统。

参 考 文 献

[1] CHAI Y P, LI T, FAN J, et al. The Connotation and Challenges of Cross-Domain Data Management[J]. Communications of the CCF, 2022, 18(11): 37-40.

[2] LAMPORT L. The part-time parliament[J]. ACM Transactions on Computer Systems, 1998, 16(2): 133-169.

[3] JUNQUEIRA F P, REED B C, SERAFINI M. Zab: High-performance broadcast for primary-backup systems[C]// IEEE/IFIP DSN. Piscataway: IEEE Press, 2011: 245-256.

[4] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]// USENIX ATC. 2014: 305-320.

[5] XU J J, WANG W, ZENG Y, et al. Raft-PLUS: improving raft by multi-policy based leader election with unprejudiced sorting [J]. Symmetry, 2022, 14(6): 1122.

[6] SAKIC E, VIZARRETA P, KELLERER W. Seer: Performance-aware leader election in single-leader consensus[J]. arXiv: 2104.01355, 2021.

[7] LIU S Y, VUKOLIĆ M. Leader set selection for low-latency geo-replicated state machine[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 28(7): 1933-1964.

[8] PARK S J, OUSTERHOUT J. Exploiting commutativity for practical fast replication[J]. arXiv: 1710.09921, 2017.

[9] MORARU I, ANDERSEN D G, KAMINSKY M. There is more consensus in Egalitarian parliaments[C]// SOSP. New York: ACM Press, 2013: 358-372.

[10] NAWAB F, AGRAWAL D, EL ABBADI A. DPaxos: managing data closer to users for low-latency and mobile applications [C]// ICMD. New York: ACM Press, 2018: 1221-1236.

[11] PU Q, ANANTHANARAYANAN G, BODIK P, et al. Low latency geo-distributed data analytics[J]. ACM SIGCOMM Computer Communication Review, 2015, 45(4): 421-434.

[12] OBASI E C M, EKE B, EGBONO F. Query Processing of Distributed Databases using an Improved GraphQL Model and Random Forest Algorithm[J]. International Journal of Scientific and Research Publications, 2022, 12(4): 454-466.

[13] NAWROCKE K, MCMANUS M, NETTLING M, et al. Query Transformations in a Hybrid Multi-Cloud Database Environment Per Target Query Performance[EB/OL]. https://www.freepatentsonline.com/y2020/0356561.html.

[14] LU L, WANG W, WANG D. A query optimization method for distributed database.

[15] DONG L, CHU A K, LIU F K. DDQO: An Algorithm for Distributed Database Query Optimization[C]// Proceedings of the 4th International Conference on Big Data and Computing. 2019.

[16] LIN Z F, YI W F, SHI G, et al. Distributed query engine and relational database query method thereof.

[17] ZHANG Q, LI J, ZHAO H, et al. Efficient Distributed Transaction Processing in Heterogeneous Networks[J]. Proceedings of the VLDB Endowment, 2023, 16(6): 1372-1385.

[18] YAN X N, YANG L G, ZHANG H B, et al. Carousel: Low-Latency Transaction Processing for Globally-Distributed Data [C]// Proceedings of the 2018 International Conference on Management of Data, SIGMOD Conference. ACM, 2018: 231-243.

[19] MU S, NELSON L, LLOYD W, et al. Consolidating Concurrency Control and Consensus for Commits under Conflicts[C]// 12th USENIX Symposium on Operating Systems Design and Implementation. 2016: 517-532.

[20] SUJAYA M, FAISAL N, DIVY A, et al. Unifying Consensus and Atomic Commitment for Effective Cloud Data Management [J]. Proceedings of the VLDB Endowment, 2019, 12: 611-623.

[21] ZHANG I, SHARMA N R, SZEKERES A, et al. Building consistent transactions with inconsistent replication[C]// Proceedings of the 25th Symposium on Operating Systems Principles. ACM, 2015: 263-278.

[22] REN K,LI D,ABADI D J. Slog:Serializable,low-latency,geo-replicated transactions[J]. Proceedings of the VLDB Endowment,2019,12(11):1747-1761.

[23] JIA X F,GAO S,ZHOU Y,et al. A data efficient cross-domain circulation technology framework for megacity governance [J]. Frontiers in Data and Computing,2023,5(5):35-45.

[24] STONEBRAKER M,BRUCKNER D,ILYAS I F,et al. Data Curation at Scale:The Data Tamer System[C]// Biennial Conference on Innovative Data Systems Research(CIDR). Asilomar,CA,USA,2013.

[25] TANG N,FAN J,LI F Y,et al. RPT:Relational Pre-trained Transformer Is Almost All You Need towards Democratizing Data Preparation[J]. PVLDB,2021,14(8):1254-1261.

[26] TU J T,FAN J,WANG P,et al. Unicorn:A Unified Multi-Tasking Model for Supporting Matching Tasks in Data Integration [C]// Proceedings of the ACM on Management of Data. 2023.

[27] TU J H,FAN J,TANG N,et al. Domain Adaptation for Deep Entity Resolution[C]// SIGMOD. 2022:443-457.

[28] WANG P F,ZENG X C,CHEN L,et al. PromptEM:Prompt-tuning for Low-resource Generalized Entity Matching[J]. PVLDB,2022,16(2):369-378.

[29] XIE T B,WU C H,SHI P,et al. UnifiedSKG:Unifying and Multi-Tasking Structured Knowledge Grounding with Text-to-Text Language Models[C]// EMNLP. 2022:602-631.

[30] ZHU M P,RISCH T. Querying combined cloud-based and relational databases[C]// 2011 International Conference on Cloud and Service Computing. 2011.

[31] DEWITT D J,HALVERSON A,NEHME R,et al. Split Query Processing in Polybase[C]// ACM SIGMOD. 2023:1255-1266.

[32] ABOUZEID A,BAJDA-PAWLIKOWSKI K,ABADI D,et al. HadoopDB:an architectural hybrid of MapReduce and DBMS technologies for analytical workloads[J]. PVLDB,2009,2(1):922-933.

[33] ARMBRUST M,XIN R S,LIAN C,et al. Spark SQL:Relational Data Processing in Spark[C]// ACM SIGMOD. 2015:1383-1394.

[34] JENNIE D,AARON J E,MICHAEL S,et al. The BigDAWG Polystore System[J]. ACM SIGMOD Record,2015,44(2):11-16.

[35] Google. Cloud Dataprep[EB/OL]. https://cloud.google.com/dataprep.

[36] HEER J,HELLERSTEIN J M,KANDEL S. Predictive interaction for data transformation[C]// Biennial Conference on Innovative Data Systems Research(CIDR). 2015.

[37] STONEBRAKER M,BRUCKNER D,ILYAS I F,et al. Data Curation at Scale:The Data Tamer System[C]// Biennial Conference on Innovative Data Systems Research(CIDR). 2013.

[38] GUO Z H,WU K,YAN C,et al. Releasing Locks As Early As You Can:Reducing Contention of Hotspots by Violating Two-Phase Locking[C]// Proceedings of the 2021 International Conference on Management of Data(SIGMOD'21). Association for Computing Machinery,New York,NY,USA,2021:658-670.

[39] WANG L,NEAR J P,SOMANI N,et al. Data Capsule:A New Paradigm for Automatic Compliance with Data Privacy Regulations[J]. arXiv:1909.00077,2019.

[40] WANG L,KHAN U,NEAR J P,et al. PrivGuard:Privacy Regulation Compliance Made Easier[C]// USENIX Security Symposium. 2022:3753-3770.

[41] ARACHCHILAGE N A G,NAMILUKO C,MARTIN A. A taxonomy for securely sharing information among others in a trust domain[C]// 8th International Conference for Internet Technology and Secured Transactions(ICITST-2013). IEEE,2013:296-304.

[42] LIN G,BIE Y,LEI M. Trust Based Access Control Policy in Multi-domain of Cloud Computing[J]. Journal of Computational and Applied Mathematics,2013,8(5):1357-1365.

[43] TANG B,SANDHU R. Extending openstack access control with domain trust[C]// Network and System Security:8th International Conference. Springer International Publishing,2014:54-69.

[44] BHATTI R,BERTINO E,GHAFOOR A. A trust-based context-aware access control model for web-services[J]. Distributed and Parallel Databases,2005,18:83-105.

[45] GRIFFIN J L,JAEGER T,PEREZ R,et al. Trusted virtual domains:Toward secure distributed services[C]// HotDep. 2005:12-17.

[46] AWAN K A,DIN I U,ALMOGREN A,et al. Robusttrust—a pro-privacy robust distributed trust management mechanism for internet of things[J]. IEEE Access,2019,7:62095-62106.

[47] BINJUBEIR M,AHMED A A,ISMAIL M A B,et al. Comprehensive survey on big data privacy protection[J]. IEEE Access,2019,8:20067-20079.

[48] CHEN D,ZHAO H. Data security and privacy protection issues in cloud computing[C]// 2012 International Conference on Computer Science and Electronics Engineering. IEEE,2012:647-651.

[49] BENANTAR M. Access control systems:security,identity management and trust models[M]. Springer Science & Business Media,2005.

[50] YAWALKAR P M,PAITHANKAR D N,PABALE A R,et al. Integrated identity and auditing management using blockchain mechanism[J]. Measurement:Sensors,2023,27:100732.

[51] WANG Z,WEI K,JIANG C,et al. Research on productization and development trend of data desensitization technology[C]// 2021 IEEE 20th International Conference on Trust,Security and Privacy in Computing and Communications(TrustCom). IEEE,2021:1564-1569.

[52] SAMARATI P,DE VIMERCATI S C. Access control:Policies,models,and mechanisms[M]// International School on Foundations of Security Analysis and Design. Berlin:Springer,2000:137-196.

[53] THAMBIRAJA E,RAMESH G,UMARANI D R. A survey on various most common encryption techniques[J]. International Journal of Advanced Research in Computer Science and Software Engineering,2012,2(7):226-233.

[54] RABAH K. Theory and implementation of data encryption

standard: A review[J]. Information Technology Journal, 2005, 4(4): 307-325.

[55] NADEEM A, JAVED M Y. A performance comparison of data encryption algorithms[C]// 2005 International Conference on Information and Communication Technologies. IEEE, 2005: 84-89.

[56] ACAR A, AKSU H, ULUAGAC A S, et al. A survey on homomorphic encryption schemes: Theory and implementation[J]. ACM Computing Surveys(CSUR), 2018, 51(4): 1-35.

[57] GONG L, ZHANG L, ZHANG W, et al. The application of data encryption technology in computer network communication security[C]// AIP. 2017.

[58] GOSHWE N Y. Data encryption and decryption using RSA algorithm in a network environment[J]. IJCSNS, 2013, 13(7): 9.

[59] HACIGUMUS H, IYER B, MEHROTRA S. Providing database as a service[C]// IEEE ICDE. 2002: 29-38.

[60] ANTONOPOULOS P, ARASU A, SINGH K D, et al. Azure SQL database always encrypted[C]// ACM SIGMOD. 2020: 1511-1525.

[61] ANSARI M D, GUNJAN V K, RASHID E. On security and data integrity framework for cloud computing using tamper-proofing[C]// ICCCE. 2021: 1419-1427.

[62] YANG J, WEN J, JIANG B, et al. Blockchain-based sharing and tamper-proof framework of big data networking[J]. IEEE Network, 2020, 34(4): 62-67.

[63] JIAO T, SHEN D R, NIE T Z, et al. Blockchain Database: A Queryable and Tamper-proof Database[J]. Journal of Software, 2019, 30(9): 2671-2685.

[64] ZHENG Z, XIE S, DAI H N, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[65] KOLESNIKOV V. Truly efficient string oblivious transfer using resettable tamper-proof tokens[C]// TCC. 2010: 327-342.

[66] BUCHMANN J, DAHMEN E, SZYDLO M. Hash-based digital signature schemes[M]// Post-Quantum Cryptography. Berlin: Springer, 2009: 35-93.

[67] ROUHANI S, POURHEIDARI V, DETERS R. Physical access control management system based on permissioned blockchain [C]// IEEE Smart Data. 2018: 1078-1083.

[68] LI T, ZHENG K, XU K. Acknowledgment Mechanisms of Transmission Control[J/OL]. http://www.jos.org.cn/jos/article/pdf/6939.

[69] Huawei[EB/OL]. https://www.huawei.com/cn/huaweitech/publication/90/deterministric-ip-networking-dark-factory.

DU Xiaoyong, born in 1963, Ph.D, professor, doctoral supervisor, is a member and fellow of CCF (No. 05422F). His main research interests include database system, big data management and analysis, intelligent information retrieval and knowledge engineering.

(责任编辑: 何杨)