

一种面向数据资源共享的安全保障模型研究

邓曦¹, 刘福金¹, 郭晓黎¹, 唐鸣²

(1. 中国电子科技集团公司第三十研究所, 四川 成都 610041; 2. 中电科网络安全科技股份有限公司, 北京 100160)

摘要: 数据作为新型生产要素, 安全共享对企业、行业乃至国家发展具有重要意义。然而, 当前数据共享面临诸多挑战。分析了数据共享中各方的核心需求, 提出了一种数据共享安全模型, 构建了数据共享基础平台。平台围绕跨地域、跨部门、跨业务等的共享交换场景需求, 解决数据共享中来源安全可靠、交换安全可控、共享安全审计、流通安全监管、传输安全可靠、数据受控访问等问题, 对推动数据安全共享发展具备一定的参考意义。最后, 分析了数据安全共享发展趋势, 包含技术融合创新对安全共享效能的有效提升, 跨领域数据安全标准体系亟待制定等。

关键词: 生产要素; 数据资源; 安全模型; 共享插件; 信任服务体系

中图分类号: TP309

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2025.10.008

引用格式: 邓曦, 刘福金, 郭晓黎, 等. 一种面向数据资源共享的安全保障模型研究[J]. 网络安全与数据治理, 2025, 44(10): 46-53.

Research on a security assurance model for data resource sharing

Deng Xi¹, Liu Fujin¹, Guo Xiaoli¹, Tang Ming²

(1. The 30th Research Institute of China Electronics Technology Group Corporation, Chengdu 610041, China;

2. CETC Cyberspace Security Technology Co., Ltd., Beijing 100160, China)

Abstract: As a new type of production factor, secure sharing of data is of great significance to the development of enterprises, industries, and even the country. However, data sharing faces many challenges currently. This paper analyzes the core requirements of all parties in data sharing, proposes a data sharing security model, and constructs a data sharing infrastructure platform. The platform revolves around cross-regional, cross-department, cross-business sharing and exchange scenarios, addressing issues such as source security and trustworthiness, security and controllability in sharing, security auditing in sharing, security supervision in circulation, transmission security and reliability, and controlled access to data, which has certain reference for promoting the development of data security sharing. Finally, this article analyzes the development trend of data security sharing, including the effective improvement of security sharing efficiency through technological integration and innovation, and the urgent needs to develop a cross-domain data security standard system, etc.

Key words: production factors; data resources; security model; sharing plugin; trust service system

0 引言

数据已经成为数字经济发展的关键生产要素^[1]。数据作为生产要素, 只有在积聚融合、交易流通、开放共享中才能发挥更大的价值^[1-2]。对于企业, 数据要素价值化能促进业务协同, 提升运营效率, 增强市场竞争力; 对于行业, 数据要素价值化有助于打破信息壁垒, 推动行业创新与发展; 对于国家, 数据要素价值化对于提升国家治理能力, 提升部门协同办公效率, 保障国家安全具有重要意义。

数据要素价值化的基础是数据能安全共享交换。然

而, 数据安全共享却面临一定的风险和隐患。一是缺乏数据共享和开放统一评估的依据, 二是缺乏界定共享责任边界的支撑手段, 三是缺乏多维度的共享全过程监管机制, 由此带来数据滥用、权属不清、责任不明等安全风险, 从而导致不愿共享、不敢共享。

数据安全共享旨在确保数据在共享过程中的保密性、完整性与可用性。本文研究了数据资源共享的核心安全需求, 建立了数据资源共享安全模型, 深入、全面分析其架构、功能和运行机制, 展示了平台模型的应用案例。从理论意义上, 通过该平台研究, 进一步完善数据安全

共享领域理论体系,为后续相关研究提供理论支撑。从实践意义上,为数据安全共享能力建设提供可借鉴参考的解决方案,有助于指导企业、行业及国家构建更安全、高效的数据共享交换平台,推动数据资源的合理流通与利用,提升整体数据安全保障能力。

1 现有研究

近年来,国内外在数据安全共享平台研究方面取得诸多成果。文献[3]建立了基于区块链的数据安全共享平台,采用区块链技术,基于哈希算法的数据加密,实现数据隐私保护、安全访问及权限控制,并实现了跨地域、跨主体、跨系统间的数据安全共享。文献[4]提出了一种基于隐私计算的政务数据共享模型,基于同态加密技术构建隐私算法服务系统,集成数据交换系统、业务服务系统等,构建了数据共享模型,以“可用不可见”的方式进行数据共享,实现数据价值的提取与共享。文献[5]提出了一种分布式云环境下的数据安全共享架构设计,基于区块链特点,解决分布式云环境的数据可信问题,基于联邦学习的数据可用不可见,解决数据孤岛和数据泄露等问题。由此可见,以联邦学习、安全多方计算为代表的隐私计算,以及区块链技术,是目前数据安全共享中的主流技术。但隐私计算主要实现数据“可用不可见”,无法实现数据资源安全地自由流通和共享。现有方案中,鲜有将区块链技术与信任技术融合,结合数据安全插件等轻量化安全技术,实现数据的自由流通、受控访问和追溯审计。

2 数据资源共享核心需求

数据作为一种资源,在流通共享过程中,一般参与方包括数据提供方、数据使用方、平台服务方、平台管理方和监管方。针对数据提供方,一是要对数据进行分类分级,做到提供数据的密级和种类底数清晰;二是要对数据进行安全存储,防止非授权的访问、窃取和篡改;三是要对数据进行泄露防护,做到敏感数据外发的监测和管控。针对平台服务方,要保障数据传输安全和数据受控交换。针对平台管理方,要保障交换实体可信、交换行为可查、攻击行为可见。针对数据使用方,要保障数据真实可信。同时,按照《中华人民共和国数据安全法》要求:“主管部门要承担本行业、本领域数据安全监管职责”。因此,数据安全共享过程,如需要受到监管的,针对监管方,要确保数据安全责任清晰,数据流转全程可查并且合法合规,安全责任可溯源定位。因此,根据在数据流通共享过程中,数据提供方、平台服务方、数据使用方、监管方不同的安全需求,建立数据资源共享核心安全需求模型,如图1所示。

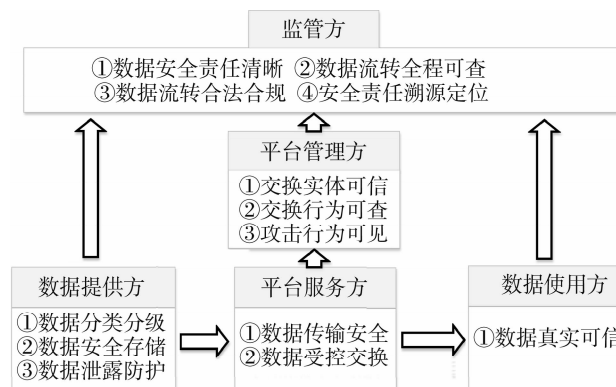


图1 数据资源共享核心安全需求

3 数据资源共享安全模型

基于数据资源共享的核心需求,本文构建数据资源共享安全模型。模型由数据提供集成、平台服务、数据使用集成、共享管理、数据资源共享融合基础设施(区块链服务、信任服务设施)、监管平台等部分组成。其中,数据提供集成将可接入的数据进行加密和打标,并完成登记和注册后,接入平台服务。平台服务提供共享平台,并提供数据资源目录、安全共享服务、安全共享管理和系统安全审计。数据使用集成通过资源门户,按照数据使用范围及获取方式,以鉴权脱标、鉴权阅读等方式,申请所需的数据资源。共享管理系统通过向数据提供集成和数据使用集成下发策略,确保数据提供时的接入控制权限、数据使用时的访问浏览权限等数据使用权限,并按要求开展共享管理控制。此外,信任服务设施和区块链设施作为基础设施,信任服务设施提供身份管理、可信时间等服务,区块链设施提供数据共享记录账本和数据鉴权决策服务。最后,数据共享监管通过数据提供集成、数据使用集成、共享管理等各方上报的监管数据,开展数据资源共享安全监管。数据资源共享安全模型如图2所示。

4 主要系统及关键技术分析

基于数据资源共享安全模型,其主要系统包括数据共享安全插件、数据资源共享融合基础设施(含信任服务设施及区块链服务设施)、数据安全共享交换系统、数据安全共享管理系统四大部分。面向数据监管方,还包括数据资源共享交换监管系统。其中的关键技术主要包括区块链技术、信任服务体系等。

4.1 数据共享安全插件

数据共享安全插件作为数据桥接与共享的安全保护系列插件,分别轻量化部署在数据提供集成和数据使用集成中,实现安全标签打标与验标、业务数据透明对接

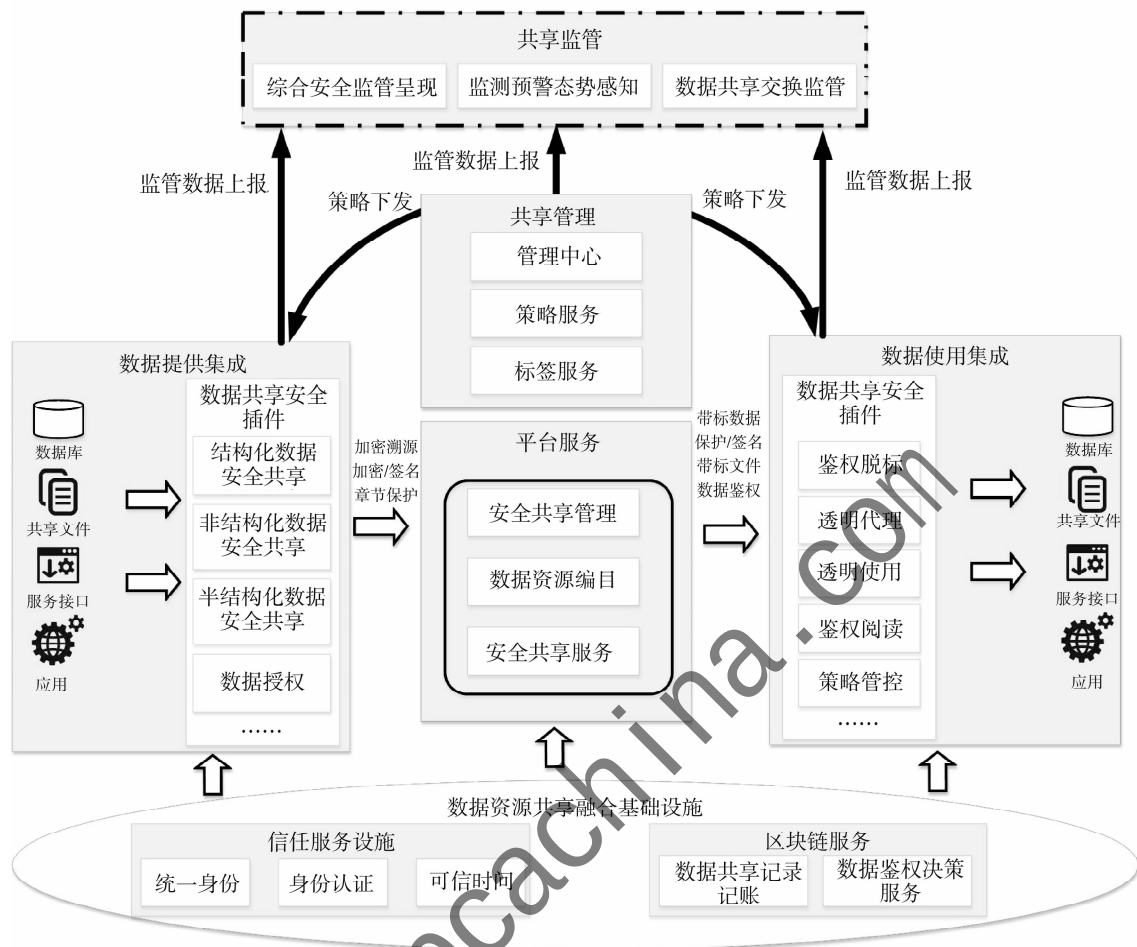


图2 数据资源共享安全模型

等。同时，依据平台服务方的安全共享管理模块，接收并执行安全共享策略。数据共享安全插件按实际使用场景中库表数据、电子文件、Web服务等，通过封装标签数据，提供分级保护、细粒度权限管控和数据确权溯源等。围绕不同使用场景，大致分为三类数据共享安全插件：结构化数据（库表类）共享安全插件、非结构化数据（文件类）共享安全插件、半结构化数据（服务接口类）共享安全插件。针对结构化数据，共享安全插件可实现：①获取数据源信息；②抽取库表数据；③提供库表数据分级保护；④标记并封装数据库表；⑤提供数据库表、列级的细粒度管控；⑥提供打标、脱标等状态信息上报。针对非结构化数据，共享安全插件可实现：①开展文件源配置；②开展使用范围、使用时间、使用频率等文件策略管控；③开展文件脱标后基于安全策略的权限验证；④开展业务访问时的文件透明脱标验证；⑤开展文件在线预览，防止数据复制或拷贝；⑥开展文件预览时的水印显示；⑦开展打标、脱标等状态信息

上报。针对半结构化数据，共享安全插件可实现：①开展接口地址、参数等安全配置；②开展应用透明化安全代理；③开展调用过程身份认证；④开展接口传输保护；⑤开展基于调用频率的接口管控；⑥开展打标、脱标等状态信息上报。面向不同应用场景，针对具体需求，部署对应安全插件，优化技术架构，实现轻量化部署。数据共享安全插件及其主要功能如图3所示。

数据共享安全插件分别轻量化部署在数据提供方和数据使用方，具体原理如图4所示。

图4所示是非结构化数据共享安全插件的具体部署及使用场景。图4（a）中，非结构化数据共享安全插件对文件/文件夹进行分类分级、分级加密和权限管控等，数据使用方基于非结构化数据共享安全插件进行授权提取，并对文件进行浏览或下载。图4（b）中，非结构化数据共享安全插件对明文进行加密保护，并根据不同应用系统权限，实现细粒度访问控制。如应用系统1具备读写权限，应用系统2具备查询权限，应用系统3不具备

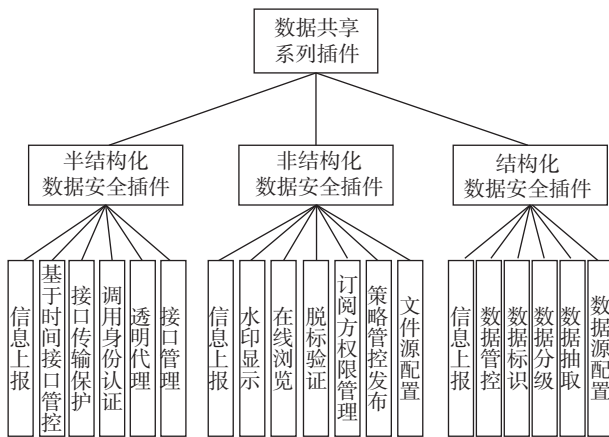


图3 面向不同应用场景的数据共享安全插件

查询或读写权限。

4.2 数据安全共享基础设施

本节将介绍实现数据资源共享过程中的身份认证、受控交换、数据防篡改，以及共享数据资源的可审计、抗抵赖的数据资源共享服务基础设施。

文献[6]中提出引入CP-ABE，指定访问权限，实现细粒度访问控制。本文基于区块链数据共享还需补强基于身份认证的细粒度访问控制能力的思路，引入信任

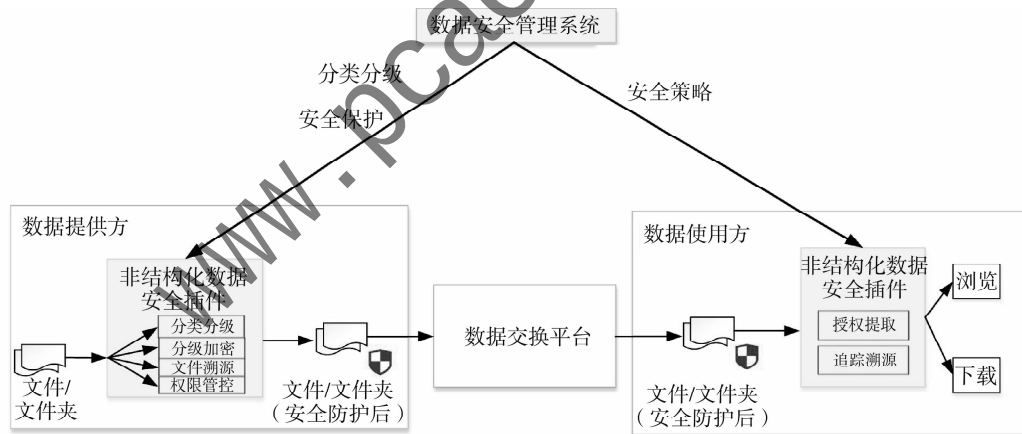
服务设施，实现基于身份属性的访问控制并对数据共享全流程中用户行为轨迹进行安全评估和安全审计，记录数据全流程各环节业务发生时间，并对数据共享各系统进行时间同步，确保数据产生的时间及内容完整。

其中，信任服务设施，通过资源管理、授权管理、身份认证和访问控制，实现信任服务、管控服务和密码服务，为数据流通共享提供基于用户身份和密码特征的细粒度访问权限控制。同时，安全审计为数据资源共享进行交换监控、行为审计和责任追溯。

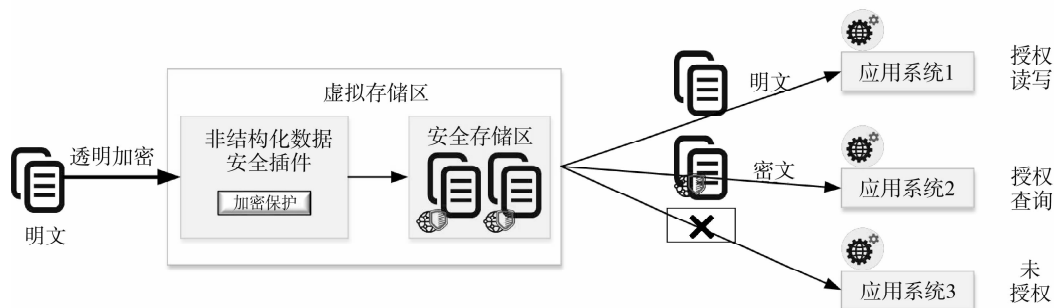
基于链式账本的服务系统记录数据资源的所有共享信息。通过维护数据块的链式结构，记录持续增长且不可篡改的数字记录。借助区块链不可篡改交易记录的特性，解决数据资源共享中电子存证记录无法自证的问题^[7]。

信任服务设施融合链式账本服务系统，不仅能实现数据共享可追溯，还可实现基于身份认证的细粒度访问控制，有效提升多用户场景下数据共享的安全性。数据资源共享下的融合基础设施架构图如图5所示。

同时，信任服务设施融合链式账本服务系统的基础设施可采用服务化架构，对基础设施层设施进行统一的服务化封装，以统一服务接口，为数据共享中数据提供方、数据使用方、信息共享交换平台等提供信任服务、



(a) 基于非结构化数据共享安全插件的文件浏览与下载



(b) 基于非结构化数据共享安全插件的权限管控

图4 非结构化数据共享安全插件的应用

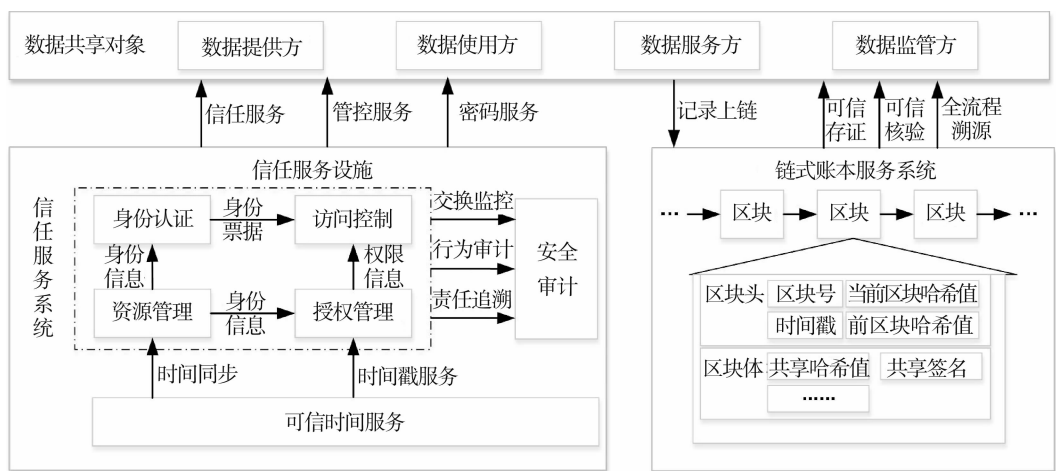


图5 数据资源共享融合基础设施

可信存证、可信时间、全流程溯源等,如图6所示。通过标准化服务接口,增强基础设施的可扩展性和弹性,简化数据资源共享基础设施的集成、使用和维护,方便数据共享各方复用平台,实现资源集约利用并降低运维成本。

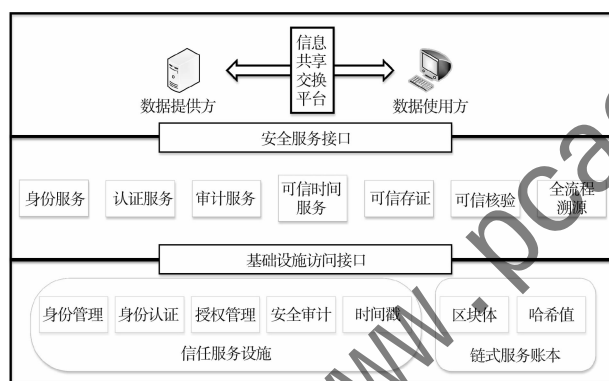


图6 数据共享安全服务统一接口示意图

4.3 数据共享交换系统

数据共享交换由共享资源目录系统和数据共享交换系统组成。数据共享交换架构如图7所示。

其中,目录系统由安全共享服务模块、安全共享管理模块、数据资源编目模块组成。安全共享服务模块提供数据检索、统计和订阅等服务;安全共享管理模块完成目录注册、审核、发布等管理功能;数据资源编目模块完成共享数据目录编制相关工作。目录系统将种类复杂、格式各异的海量数据,基于异构数据共享模型,建立规范的映射逻辑空间,将不同类型的异构数据存放在相应空间中,实现数据与对应业务应用的匹配,形成异构数据的互联互通和高效管控。

安全共享交换系统由数据交换服务模块和数据共享

安全插件模块组成。其中,数据共享安全插件模块可部署在数据提供方和数据使用方,也可以部署在数据共享交换软件中。数据共享安全插件已在4.1节进行了介绍,不再赘述。

数据交换服务模块包含5大功能:(1)开展数据分类、共享机构、热门数据排行等信息展示和共享数据检索;(2)对交换数据进行基于标签的规则检查,按照安全策略对交换数据进行管控;(3)需包含对数据库、文件、音视频等多样化的文件支持;(4)具备支持点对点、一对多、多对多、发布订阅等多种交换方式;(5)支持库表、文件、数据流等多种数据类型的接入。

4.4 数据安全共享管理系统

本文设计的数据安全共享管理系统由数据共享交换管理、数据安全标签管理、数据安全策略管理等组成,提供数据安全配置管理和服务功能,包括策略决策、下发与查询等。数据安全共享管理系统通过向数据共享安全插件下发策略、标签打标和标签验证,实现基于权限的数据访问控制。数据安全共享管理系统功能框图如图8所示。

数据共享交换管理为结构化、非结构化、半结构化数据提供数据分类分级配置、安全策略配置、安全防护配置、数据标签管理、流转溯源管理、数据泄露管理、系统管理等,开展集中统一的数据源管理、数据安全分类分级、数据分级保护和细粒度数据安全策略制定及下发。

数据安全标签管理提供数据标记、数据脱标、标签完整性验证等接口服务,提供数据标、分离标等多种数据标签封装,提供标记数据的鉴权提取功能,支持商用密码、同态加密等算法,提供数据机密性、完整性、不可否认性保护。

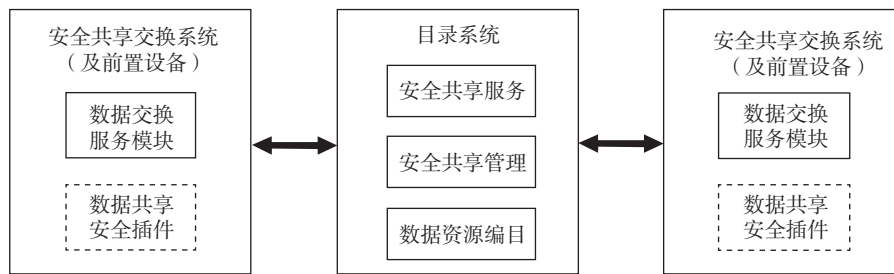


图7 数据共享交换架构图

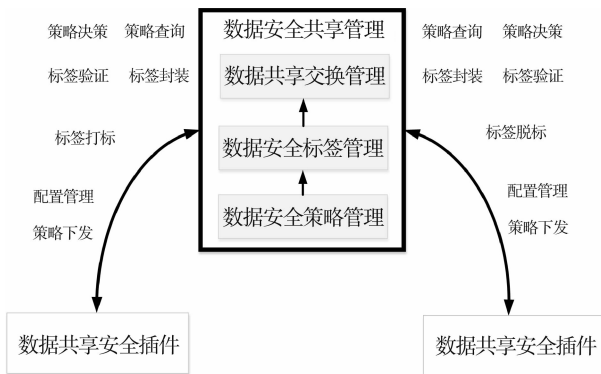


图8 数据安全共享管理系统功能组成图

数据安全策略管理提供数据安全策略查询、安全策略下发等安全策略服务，提供支持基于区块链实现数据鉴权共享的服务，提供支持策略服务集群、策略服务分布式部署等弹性服务，提供支持安全策略推送给数据安全标签的安全策略管理服务。

针对上述3个管理系统，数据安全标签管理涉及对数据提供方和数据使用方的数据开展基于标签的访问控制。数据安全标签管理按照数据的重要程度、标记主体、安全策略等信息形成数据安全标签，具备数据标签的标签生成、标签修改、标签识别、标签验证、标签提取、标签跟踪、标签使用，以及应用授权、应用认证、标签服务中间件等功能。标签管理对文件夹、文件、数据库进行标签生成和标签修改，跟踪数据流转状态，联合数据共享交换监管系统，协助实现事后追责。

4.5 数据共享交换监管系统

数据共享交换监管系统是面向第三方监管需求设计形成的系统。根据我国相关法律规定，监管机构及企业自身需要掌握企业数据流通共享情况，及时发现企业数据安全行为。重要数据处理活动需加强风险监测，定期开展风险评估。因此，针对数据流通共享过程中监管方的需求，需建立数据共享交换监管系统，满足流通共享数据备案、监测分析、安全预警、统计展示和责任认定

等功能，为监管方提供抓手级服务平台和监管服务，促进数据要素合规流动。数据共享交换监管系统模型如图9所示。

在数据共享交换监管系统中，监管系统收集数据提供方、数据使用方、共享交换业务系统、基础设施等管控对象的基础日志和标签日志信息，对交换节点进行实时监控。基于上述日志及信息，开展安全分析、协查取证和态势呈现，为监管机构掌握数据流通共享情况提供监测信息、统计展示和溯源取证等。

5 应用案例

根据本文对数据资源共享的安全保障模型研究结果，某业主方建立了信息共享交换安全防护平台，针对平台管理，部署了数据安全管理系统，另外提供区块链服务、密码服务和信任服务。针对共享监管，部署了数据安全共享监管系统。针对数据提供方和数据使用方，分别部署业务中台和数据共享插件。通过系统部署，实现了对业务文件的加密传输和基于权限的访问控制，并实现流转过程的详细记录，保障了数据可用、可管、可控。应用案例的详细部署如图10所示。

针对数据共享，数据提供方基于数据共享安全插件，对共享数据进行分类分级和分级加密；数据安全共享管理系统开展数据打标、数据共享、策略下发等；数据使用方基于数据共享安全插件，按照“权限控制”下发策略，对共享数据进行授权解密和脱标，实现数据安全流通和基于身份认证的细粒度访问操作控制。

其中，场景1中，业务系统1由于未收到下发策略，无法查看和读取文件；业务系统2收到“授权查询”下发策略，能查看文件；业务系统3收到“授权读写”下发策略，能查看和修改文件。场景2中，对库表文件进行了加密传输，数据使用方通过“授权使用”下发策略，对库表文件进行提取，实现库表文件安全共享。场景3中，对Word文档进行共享，基于数据共享安全插件收到的“不同权限”下发策略，不同用户只能查看符合其权限的内容，实现内容管控。另外，基于时间源，对所有

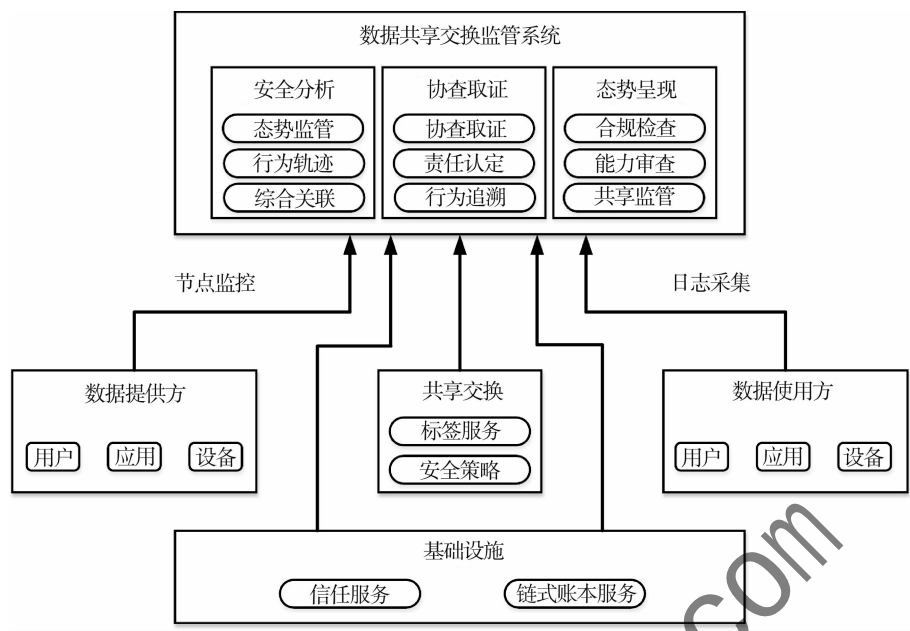


图 9 数据共享交换监管系统模型

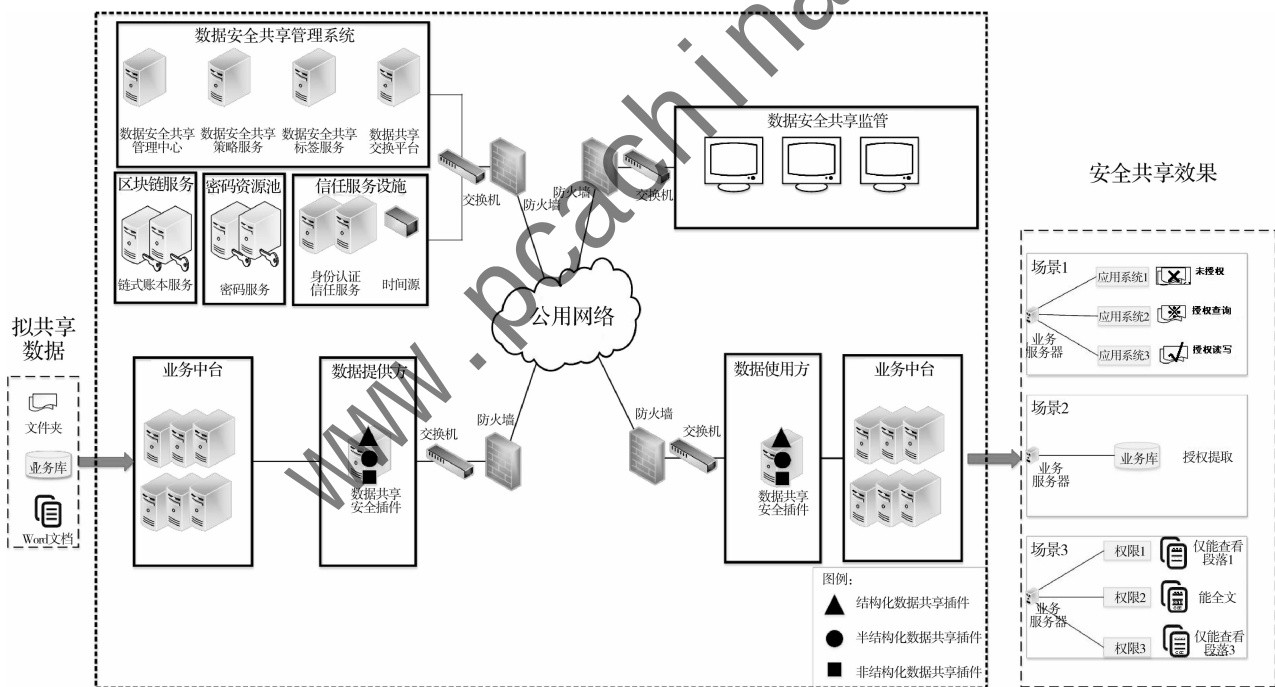


图 10 数据资源共享安全保障应用案例

操作行为进行了时间同步和记录管理。

最后，共享数据的分类、分级、名称、所属机构、操作时间、流转总量等信息都在数据安全共享监管系统上展示，满足了主管部门在本领域的数据安全监管职责要求。

6 发展趋势分析

6.1 新技术对数据安全共享的影响

随着数据资源共享技术不断发展，单一的安全技术已难以满足复杂多变的安全需求，未来多种安全技术将走向融合，形成更高效的安全保障机制。如人工智能能与区块链技术的结合，具有巨大的潜力^[8-9]。人工智能凭借其强大的数据分析与学习能力，提升区块链系统精准识别和威胁应对能力。同时，通过对区块链上大量共享数据的深度分析，人工智能算法能及时、有效、全面地发现异常行为模式，提前预警共享基础设施可能的安全风险。

险,增强防御能力。最后,区块链的不可篡改性和分布式账本特性可为人工智能提供可靠的数据来源,确保训练数据的真实性和完整性,提升人工智能模型的准确性和可信度。

另外,加密技术与访问控制技术的融合也将成为趋势。先进的加密技术可对数据在共享过程中的各个环节进行加密保护,精细化的访问控制则能够依据用户的身份、权限等因素,严格限制对加密数据的访问操作。例如,通过软件定义边界(SDP)技术,隐藏数据资源网络地址,仅允许通过身份验证的用户通过加密隧道访问指定端口的数据。对API调用实施零信任,通过多因素认证机制验证请求身份,结合流量分析与行为分析,动态调整API访问权限,防止API滥用或恶意爬取数据。

6.2 跨领域安全保障体系协同发展

未来,不同领域的的数据资源共享将日益频繁,但各个领域数据特点和安全需求存在差异,安全保障体系各不相同,需加强不同领域数据资源共享的安全协同保障体系构建,形成面向不同领域的统一安全标准和管理模式。例如,在医疗与金融领域的的数据共享中,医疗数据注重患者隐私保护,金融数据则强调交易安全与资金保障。通过协同体系构建,可制定一套兼顾两者需求的安全标准,确保在数据共享过程中既有效保护患者隐私,又保障金融交易安全可靠。同时,还需要建立统一的跨领域安全共享平台,对跨领域数据共享进行集中监控与管理,促进海量异构数据安全地在不同领域间顺畅流动、高效利用。

7 结论

数据安全共享是发展数字经济的前提,本文针对数据流通后数据会脱离数据所有者的控制这一数据共享的根本问题,立足数据作为资源要素,从流通共享的安全需求出发,提出了一种数据资源共享的安全保障体系,涵盖了数据提供方、数据使用方、数据监管方等不同责任主体的安全需求,开展了以数据为中心的体系化安全防护,确保了数据在流通过程中可感、可控、可管,可为数据资源多方共享利用提供参考。

未来,面向多领域融合数据安全共享,如面向健康数据共享与精准医疗、数据安全协作与智能制造、供应链系列环节数据共享、多源数据融合与公共服务优化等具体应用场景,一是还需补强零信任架构与动态访问控

制。本文中的信任体系主要基于传统信任设施,开展静态授权,下一步需结合新兴技术,开展基于动态信任评估与策略执行的数据安全访问控制研究,构建更高效、可信的数据访问控制体系。二是实现AI驱动的安全智能。利用机器学习识别异常数据访问模式,动态调整安全策略,结合自然语言处理,自动解析数据共享协议,减少人工运维工作量,降低合规成本。三是构建数据共享规则体系。面对具体行业的需求和难点,制定行业标准和认证体系,解决数据确权与定价难题,明确价值分配,激发数据拥有方开展数据共享的积极性,牵引指导企业面向数据共享的合规能力建设,实现数据安全有序流动。

参考文献

- [1] 孙克. 数据要素价值化发展的思考[J]. 信息通信技术与政策, 2021, 47(6): 63-67.
- [2] 中共中央, 国务院. 中共中央 国务院关于新时代加快完善社会主义市场经济体制的意见[Z]. 2020.
- [3] 高丽. 基于区块链技术助力实现数据安全共享的研究[J]. 信息系统工程, 2024(5): 55-58.
- [4] 马英. 一种基于隐私计算的数据共享模型研究[J]. 信息安全研究, 2022, 8(2): 122-128.
- [5] 石进, 钱诗君, 沈驰, 等. 面向分布式云环境的数据安全共享架构设计[J]. 信息化研究, 2023, 49(4): 55-59.
- [6] 王贤哲. 基于CP-ABE和区块链技术的数据安全共享技术[J]. 电脑知识与技术, 2024, 20(14): 83-85.
- [7] 周斯琴. 基于区块链的医疗数据安全共享方案的设计与实现[D]. 武汉: 武汉大学, 2019.
- [8] 杨晶. 区块链赋能数据资源安全共享应用研究[J]. 中国科技产业, 2022(10): 70-72.
- [9] 刘泽雷, 胡超, 孙阳, 等. 联邦学习贡献评估在数据要素流通领域的探索与前瞻[J]. 人工智能, 2023(6): 24-34.

(收稿日期: 2025-07-09)

作者简介:

邓曦(1985-), 男, 硕士, 高级工程师, 主要研究方向: 数据安全、网络与信息安全。

刘福金(1989-), 男, 硕士, 工程师, 主要研究方向: 密码应用与数据安全。

郭晓黎(1977-), 女, 硕士, 研究员级高级工程师, 主要研究方向: 密码应用与数据安全、网络与信息安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com