基于内生安全的数据共享信息系统架构研究

李 建[1,2],王 昊[1,2],姜芳峰[1,2],罗清林[1,2],吴凡毅[1,2,3]

(1.中电(海南)联合创新研究院有限公司,海南 澄迈 571924;
2.海南省 PK 体系关键技术研究重点实验室,海南 澄迈 571924;
3.中国电子信息产业集团有限公司,广东 深圳 518057)

摘 要:在研究了我国数据共享信息化发展的阶段规律和相应架构体系变迁的基础上,结合我国数据治理法规标准体系要求和 PKS 自主计算体系发展现状,研究在可信安全计算环境中数据不脱离数据拥有方的、可主动免疫的架构设计原则、实现方案,包括底层可信的基础软硬件系统,上层应用零信任的主动审计防御体系,以及"数据拥有方主导+数据交易第三方负责的可信网络路由交换集中运维"的数据共享建设思路、建设内容、实施路径等。最后指出未来数据共享应用场景中可能面临的新风险、新问题,并提出构建符合法理要求和内生安全理念的新一代信息化架构体系的一些综合建议。

关键词:PKS 体系;数据共享;内生安全;可信计算;零信任;系统架构

中图分类号:N949;F49 **文献标识码**:A **DOI**:10.20044/j.csdg.2097-1788.2022.01.011

引用格式:李建,王昊,姜芳峰,等. 基于内生安全的数据共享信息系统架构研究[J].网络安全与数据治理,2022,41(1):70-77.

Research of data sharing information system architecture based on endogenous security

Li Jian[1,2], Wang Hao[1,2], Jiang Lifeng[1,2], Luo Qinglin[1,2], Wu Fanyi[1,2,3]

(1.CEC Joint Innovation Research Institute Co., Ltd., Chengmai 571924, China;
2.Key Laboratory of PK System Technologies Research of Hainan Province, Chengmai 571924, China;
3.China Electronics Corporation, Shenzhen 518057, China)

Abstract: Based on the study of the stage law of the development of data sharing informatization in China and the changes of the corresponding architecture system, combined with the requirements of Chinese data governance regulations and standards system and the development status of PKS independent computing system, this paper studies the architecture design principles and implementation schemes of data without breaking away from data ownership and active immunity in the trusted and secure computing environment, including the underlying trusted basic software and hardware system, the active audit defense system with zero trust applied at the upper layer, as well as the data sharing construction idea, construction content and implementation path of "Data is dominated by data owners+Centralized operation and maintenance of trusted network's routing switching dominated by the third party of data transaction". Finally, it points out the new risks and problems that may be faced in the future data sharing application scenarios, and puts forward some comprehensive suggestions on building a new generation of information architecture system that meets the legal requirements and the concept of endogenous security.

Key words: PKS system; data sharing; endogenous security; trusted computing; zero trust; system architecture

0 引言

继原始文明、农业文明、工业文明时代之后,人类已进入当今的数字文明时代。特别是大数据、人工智能、云计算、区块链等新一代信息技术的逐步成熟,加速了数字经济时代的到来,革新或颠覆了传统的经济形态,使得越来越多的国家将数字经济

www.pcachina.com

上升为国家战略，并逐步成长为世界各国经济增长的强大引擎。欧洲委员会指出，“数字经济”将数据视为“未来经济的基石”，决定着商业的成功和经济的未来繁荣[1]。整体来看，美国、英国、德国、法国、加拿大、澳大利亚等主要西方发达国家，早在20世纪60~80年代，就开始出台关于信息自由、数据保护等方面的国家层级的法律，如今已基本构建有利于数据开放利用的数据法规制度体系[2]。我国自党的十九届四中全会首次把数据与劳动、资本、土地、知识、技术、管理一并视为生产要素后，大大加快了成体系的数据立法工作。2020年3月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，明确提出“加快培育数据要素市场”，“根据数据性质完善产权性质，完善数据产权界定”，数据作为一种新型生产要素，第一次直接写入中央政策文件中；2021年，我国又颁布和实施《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》，基本构建了比较完整的数据安全治理体系，其全景图如图1所示，标志着数据安全治理领域正式进入体系化强监管时代。

1 数据共享发展概述

近年来，美国对抖音国际版TikTok进行国家安全审查等数据安全事件，以及俄乌数字安全攻防战背后体现的全域、全天候、全方位安全防护问题，警醒了我国党政军民相关主体，同时也对解决日益严峻的数据安全威胁提出了更高的要求。如何合规安全地发挥数据价值，兼顾发展和安全，平衡效率和风险，是当前面临的重要课题。习近平总书记指出，要统筹国内国际两个大局、发展安全两件大事，充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，不断做强做优做大我国数字经济[3]。

在数据进入要素化交易共享的高级发展阶段，数据作为关键的生产要素可以通过市场化配置，实现全领域、全行业、全地域、全平台机构间的数据智能流转，使得数据这种新的生产要素得以从另外的角度推动当今数字经济增长，加速释放要素价值。但数据可以轻而易举地被复制，且复制、传播几乎不需要成本，很多共享数据的优势方已经取得规模优势或绝对优势。如仍不加以法规制度约束，原先掌握大量个人和组织数据的互联网巨头(阿里、腾讯、京东、滴滴等)的数据量级还会野蛮增长，数据和平台相互依赖的风险进一步提升，很多大的数据平台

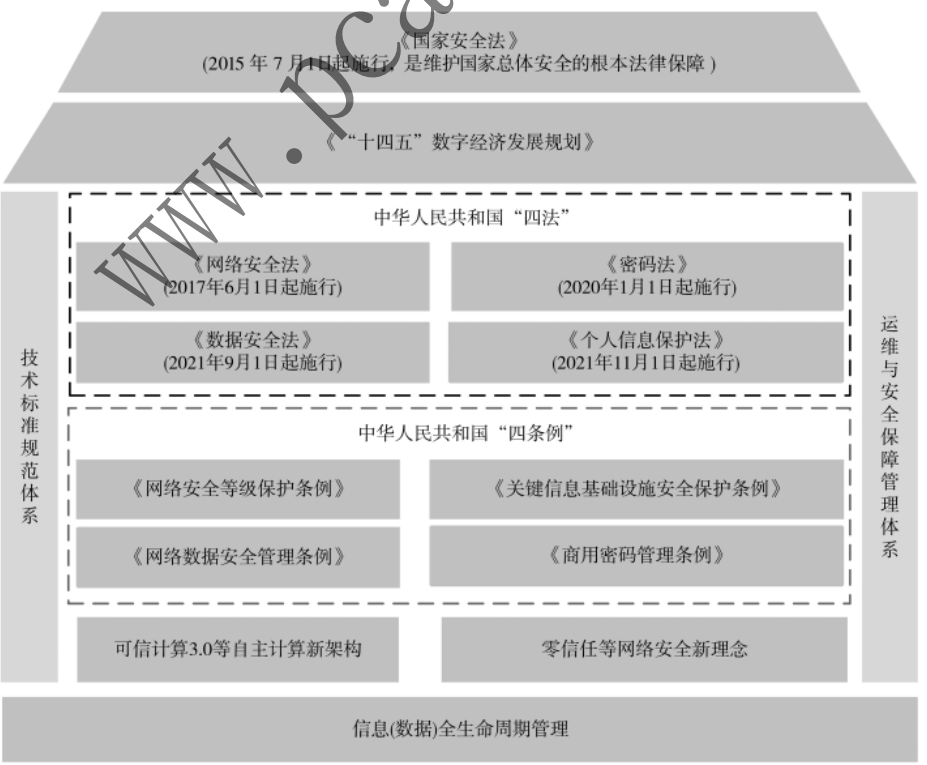

图1 数据安全治理体系架构图

www.pcachina.com

甚至能够利用已有数据创造出新的资源,进而设置壁垒,并拒绝其他厂商进入,从而形成并维持竞争优势,导致垄断风险。另外,公安等核心党政部门则存在数据合规建设问题,此类公共数据如果出现滥用,会造成更大的损害。因而建设一个符合数据安全和个人信息保护合规体系的基于内生安全理念的新型数据共享信息系统成了迫切需求。

2 基于内生安全理念的数据共享信息系统架构

2.1 现有技术基础与问题概述

现有数据共享信息系统大都基于 Wintel 体系(Microsoft Windows 操作系统+Intel CPU 组成的计算架构体系简称)的底层软、硬件来集成,包括密码机、网闸等外挂式安全设备,并采用第三方工具或自研软件进行数据识别、转换、分析与集成,然后通过远程方式连接到数据拥有方的数据库,进行数据抽取和挖掘。从技术上讲,在此安全机制下的数据共享,很多数据共享信息系统即使采用复杂的加、解密技术防护体系,底层漏洞或后门仍会带来不可控的数据安全风险,另外,外挂式安全还会降低整个系统的运行效率。从数据资产属性上讲,数据共享的前提是要保证在交换过程中对数据主权的控制[4],目前看数据主权并不可控:一是数据需求方可以获得数据拥有方数据库的部分或全部操作权限,或者直接提取相关数据,并自行存储,使得数据拥有方无法把控数据安全性,也无法发挥数据资产的价值;二是数据拥有方对自己的数据丧失管理权,不知道谁抽取了自己的数据、抽取了什么数据,多少数据,更不知道数据需求方是否进行二次开发利用,甚至私下出售原生或衍生的数据信息。

2.2 数据共享方案总体设计

数据获取、交易制度的核心和重要前提是数据权利界定规则的全面、完整、清晰,这不仅有利于明确交易对象、厘清交易成本和确立协议定价,而且对加强事后监督、降低履约成本都具有显著的价值[5]。目前在很多行业应用领域都存在数据归属鉴定及应用困难的问题,很多地方靠行政命令等强制手段实现数据共享。虽然此类数据共享也在不断创造价值,但未来发展瓶颈也很明显。以政府等公共数据为例,很多地方的大数据局虽实现了涉及婚姻、社保、教育、医疗、救助等信息的人口库,涉及工商、质监、地税、国税、社保、财政等信息的法人库,涉及“天地图”服务规划等信息的空间地理库等静态基础数据的共享,但动态数据的共享情况仍旧不是很乐观。经常是“一把手”一管就共享,不管就不共享。另外,“大厅大屏大集中”方式也存在弊端,很多地方把数据都集中起来,数据的平台化汇聚加剧了数据安全风险,形成数据的“蜜罐效应”,导致数据存储平台容易成为网络犯罪的攻击目标[6]。一旦发生数据泄露等安全事故,就是全系统泄露,因此,数据流通过程中产生的权益归属、安全保护、合规应用等问题,成为政、产、学、研、用等各界关注的焦点。

为了解决数据共享问题,且保证数据共享的安全性,本文提出基于内生安全理念进行数据共享交易方案的总体设计,如图 2 所示。

图 2 展示的参考案例中,A_1 单位需要 C_1、C_2 单位的有关数据,A_2 单位需要 C_2 单位的有关数据,A_n 单位需要 C_2、C_n 单位的有关数据。

本方案架构设计的核心是数据拥有方可以不必对外直接提供业务数据库的原生数据,而是将数据需求方的计算模型存入自己管控的可信对接总线子系统,从而解决了对共享数据的控制权问题。另外,数据需要方和数据拥有方的角色并不固定,可根据不同场景进行角色变换,现实中很多单位都具有数据需要方和数据拥有方的双重身份。该架构设计的主要技术特征:一是数据需求方先提交数据需求及用途,并向数据共享交易管理中心和数据拥有方提交计算模型全部源代码,然后进行源代码审查,审查通过后,由数据拥有方将计算模型写入可信对接总线子系统;二是数据拥有方通过数据共享交易管理中心链接数据拥有方的信息系统,并以可信应用程序接口(Application Programming Interface,API)调用等方式运行自己编写或认可的计算模型,由计算模型去抽取并分析数据拥有方业务子系统数据库的相关数据,完成计算后,再根据三方预设的安全机制,对所述计算结果进行对应的处理,得到安全计算结果或反馈信息;三是三方系统的可信部分均要求没有未知指令集和未知代码,包括基础的芯片、操作系统以及上层应用等都应具有“可知、可自主编码、可重构、可信、可用、可控”等特点。比如,基于 ARMv8 架构授权而研制的飞腾自主芯片完全符合上述要求,且具有支持国密算法等内生安全特色。同时,数据共享交易管理中心既要关注传统数据管理层面的目录管理、安全管理、质量管理,

www.pcachina.com

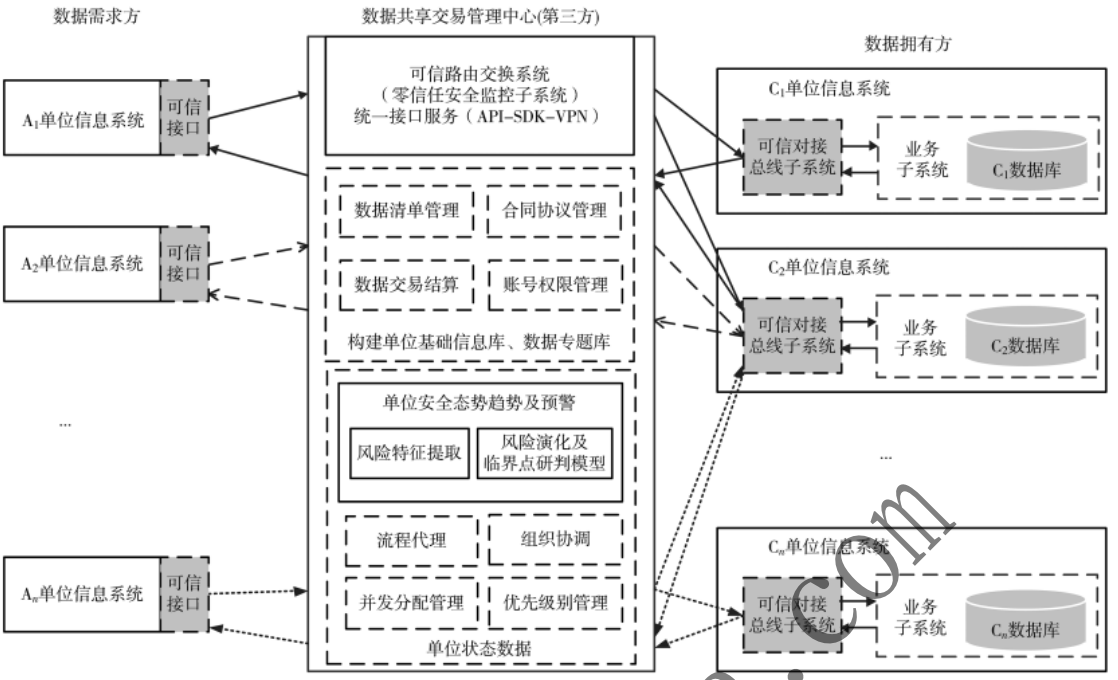

图 2　基于内生安全理念的数据共享信息系统架构总体设计

又要关注资产管理层面的数据审计、价值评估和利益分配[7]。目前，很多地方的数据交易第三方的角色由省大数据管理局等担任，其作用与价值是高效统一单位基础信息，统一接口服务，统一业务协调代理，统一数据资产计价交易，解决业务协调难、单位(系统)状态监测难、数据资产计价难等问题。

2.2.1 可信对接总线子系统的可信计算架构

沈昌祥院士指出，主动免疫是中国可信计算革命性创新的集中体现，在计算和防护双系统体系框架下，采用自主创新的对称与非对称相结合的密码体制，作为免疫基因；通过可信平台控制模块(Trusted Platform Control Module，TPCM)上主动度量控制芯片植入可信源根，在可信密码模块(Trusted Cryptography Module，TCM)基础上加以信任根控制功能，实现密码与控制相结合，将可信平台控制模块设计为可信计算控制节点，实现 TPCM 对整个平台的主动控制；在可信平台主板中增加可信度量控制节点，实现计算和可信双节点融合[8]。PKS 体系(PKS 体系是基于自主的飞腾(Phytium)中央处理器(CPU)和麒麟(Kylin)操作系统(OS)，具有双体系防护结构，具备内生内置安全能力的架构体系)正是主动免疫可信的“安全+计算”双体系架构的一种具体实现，其加载及信任链传递流程，可实现最底层、最基础、最必要的计算和安全功能的全覆盖。可信对接总线子系统的可信计算架构由底层可信基础软硬件和上层可信应用软件组成。其中 PKS 体系内置可信环境的硬件可信根可以是飞腾 CPU 可信核或 TCM 上的密码芯片，通过可信根建立内置可信信任链，并在基础软硬件可信架构体系构建完成后，运行在系统上的应用也应基于可信软件基服务完成验签流程，具体如图 3 所示。

2.2.2 零信任安全监控子系统

数据共享交易管理中心应负责可信路由交换系统建设，其中最核心的部分是零信任安全监控子系统，顾名思义，就是基于零信任理念不断对物理与环境安全、主机与存储安全、网络安全、虚拟化安全、数据安全、应用安全和用户行为安全等进行动态、无感的监控验证。该系统的设计规范应符合国家强制标准《计算机信息系统 安全保护等级划分准则》，包括在系统可信基构造时，排除那些对实施安全策略并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度；支持安全管理员职能；动态扩充审计机制，当发生与安全相关的事件时发出警告信号，提供应急处理和系统恢复机制，提高系统抗渗透能力[9]。另外，零信任安全监控子系统作为主动式防御体系的核心基石，除了具备终端环境感知、可信访问控制、可信应用安全

www.bcachina.com

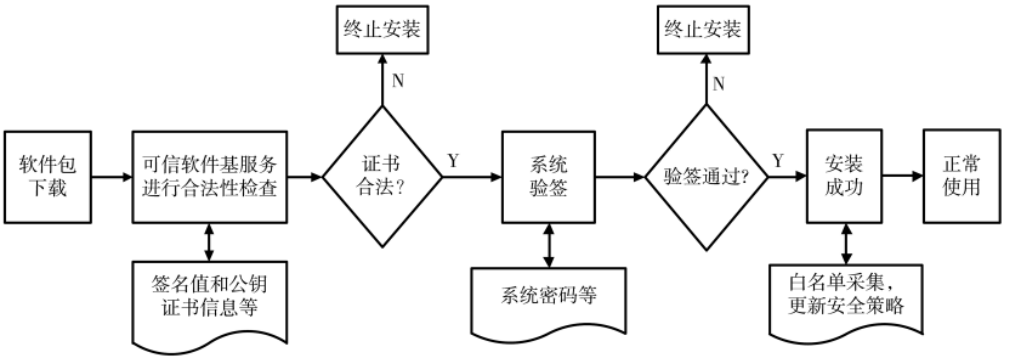

图 3 可信软件基服务验签流程图

API 监管、用户行为统计、身份认证安全审计与数据完整性流程记录管理等功能外,还应基于等保 2.0 标准和原则,着重实现具有安全免疫和主动防御能力的主机系统安全保护方案,全面提升主机系统在复杂攻击环境下的安全性能[8]。特别是要具备对系统运维管理等重点人群主动监控功能和外部多源信息响应机制,比如民众举报、舆论等外源信息。

2.2.3 数据共享申请与计算模型授权流程

数据共享申请与计算模型授权应按法理依据进行审批,具体流程如图 4 所示。

数据拥有方存储有数据需求方的计算模型,且计算模型的每次更新均需通过数据拥有方审核确认,确保数据一直内置于数据拥有方信息系统,只反馈预先商定的计算结果。数据资产不脱离原有主体,可以大幅提高数据拥有方的共享意愿,且通过搭建数据需求方可信接口或数据拥有方可信对接总线子系统,可以很好地解决原有系统的利旧问题,只需让可信接口或可信对接总线子系统和旧的信息系统对接便可,大幅提高了系统兼容性,降低了信息化项目成本。另外,在数据拥有方提供数据不共享说明的情况下,还应建立特许数据服务共享流程和机制。例如,某单位需要调研某犯罪嫌疑人的银行流水及其资产等数据,该单位应按法理依据进行审批,拿到公安司法机关给出的调查令后,由数据共享交易管理中心分发至相关数据拥有方,实现授权书(行政许可等)一对多,大幅提高了特许特批数据共享反馈的流程效率。

2.3 数据共享计算过程参考实现

数据需求方发送数据请求至数据拥有方之前,需要通过数据共享交易中心建立与数据拥有方的信道连接,因此,数据拥有方会通过可信对接总线子系统接收经数据交易中心转发且验证过的数据

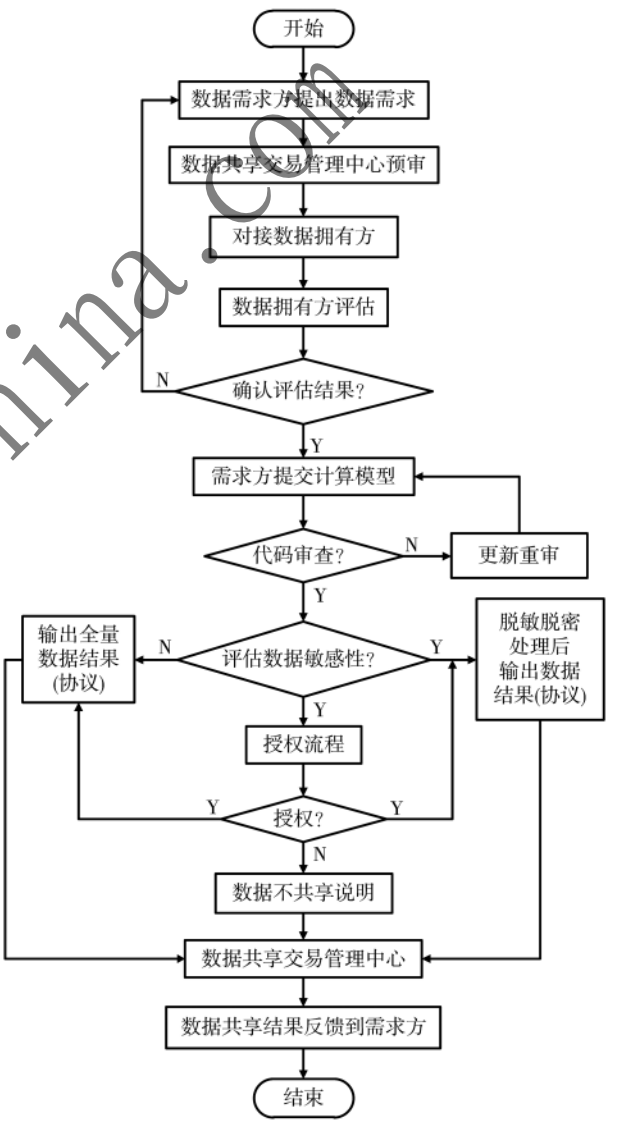

图 4 数据共享申请与计算模型授权审批流程图

需求方的访问请求,验签均通过后,建立计算模型调用链路,开始正常调用计算和结果反馈工作。数据共享计算过程参考实现如图 5 所示。

www.pcachina.com

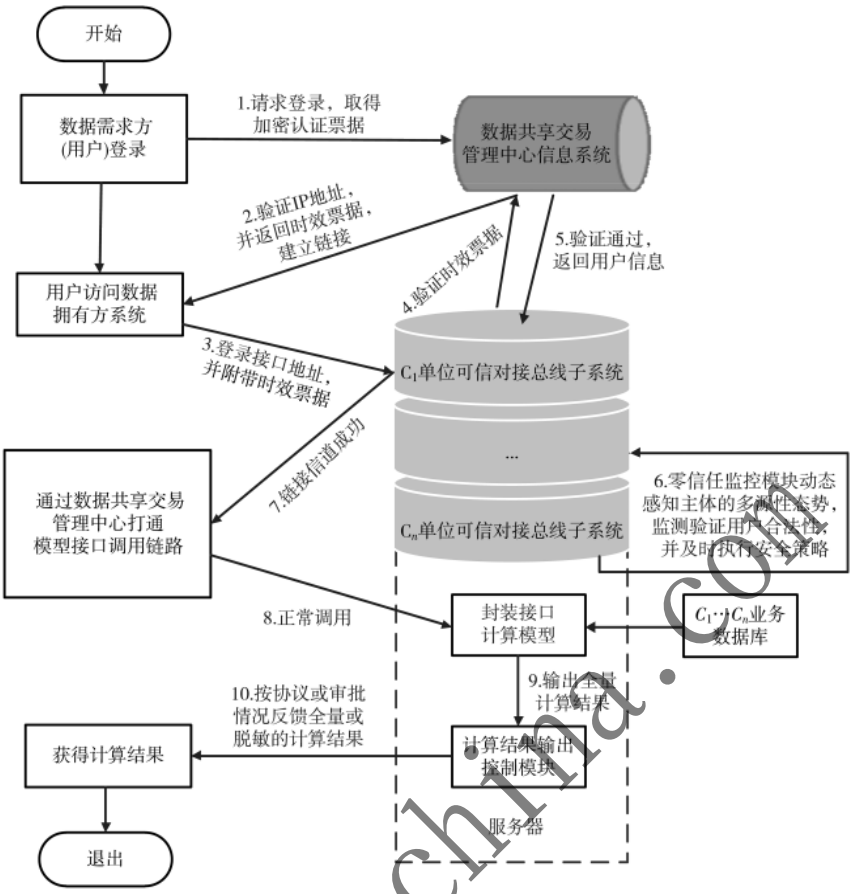

图 5　数据共享计算过程参考实现示意图

2.4 数据共享机制

数据作为生产要素释放价值的前提是构建一整套有利于数据交易流动的数据治理体制机制。以成都市政府数据授权运营为例，张会平等[10]认为政府数据授权运营机制包括运营管理监督机制、平台建设运行机制、网络安全保障机制、数据需求管理机制、数据申请与授权机制、数据交付与利用机制、利益补偿与激励机制以及数据服务定价机制，指出其基本特性是将政府数据作为国有资产进行市场化运营。除此之外，还应建立或完善数据资产交易保证机制，数据服务分类分层计价交易机制，数据共享白名单、黑名单机制等，为数据交易共享培养创新土壤。

(1)数据资产交易保证机制。建立类似互联网交易支付中介，各单位进入数据共享系统即交保证金，方便信息系统结算数据资产。

(2)数据服务分类分层计价交易机制。数据会产生存储、维护和安全等持续性管理成本，没有科学的分类分层计价机制，数据就会变相成为资产负债。一是长时间占用链路的数据服务，比如摄像头等流式数据，按照设备采购及维护费进行预期寿命内的时间分摊，并按三分之一的分摊费用计价，即当流式数据的使用客户达到 3 个时，数据拥有方即可实现零成本运维，有利于高质高效提供可持续的数据服务；二是条目式或确认式数据服务，按条目或流量计价，计价协议经双方商定后，数据交易共享中心备案落实。

(3)数据共享白名单、黑名单机制。数据共享交易管理中心应推动接入系统的相关单位建立数据共享白名单、黑名单机制，其中，数据共享黑名单要求说明不共享的理由，包括法规意见或单位条例等法理依据。

3 数据安全趋势展望与建议

在政策驱动和市场需求同时作用下，数据共享广度和深度在数字经济行业应用项目中日益加强，使得当前热门的数字政府、智慧城市等数字化项目的数据安全风险，以及未来数字战争等应用场景的预期风险也同步放大。

www.pcachina.com

3.1 完善跨境数据流动的监管组织及制度建设

《非对称竞争:应对中国科技竞争的战略》报告中的一项就是数据本地化,本地数据物理隔离。文中提出的核心政策就是将美国私营企业的科技能力整合到美国政府的军事情报战略中,同时将美国政府获得的信息应用于私营企业的经济和科技竞争中[11]。微信、抖音等大型社交平台有太多可以利用的多源数据,抖音国际版 TikTok 在美国受限的背后就是民用数据跨境之争,而对军用数据而言,军民融合多源大数据安全更为重要,数据安全攻防优势方完全可以实现局部甚至全局战场的透明化。因此,只有尽快完善跨境数据流动的监管组织及制度建设,逐步明确直接或间接传输审查的范围和阈值,才能积极参与数字经济国际合作。

3.2 闭环流转,建立数据安全全生命周期管理体系

基于我国的数据治理体系,建立覆盖数据采集、存储、共享、开放、应用、消亡等涉及数据安全的全生命周期管理体系,包括安全管理标准规范[12]等,逐步实现由事后管理向全过程管理转变,建议重点围绕数据主权问题,开展以下三方面的工作。

(1)健全关键领域私营或外资单位数据准入制度

以滴滴事件为例,大规模打车平台行程和个人数据一旦被相关民营或外资企业泄露给敌对方,平时可以轻易分析出涉及军事敏感地相关人员,如果再综合其他平台的多源数据,就可进行精准的人物画像,便于间谍渗透;战时则可能导致军事敏感地和关键人员在首轮突袭中遭受毁灭性打击。因此,应健全关键领域私营或外资单位数据准入制度,包括数据采集、共享等核心环节的审核。针对掌握规模级大数据的互联网平台或信息系统,法理上应设置相关数据的默认存储期(个人选择长期存储的除外),交易类数据应可由个人自行删除,并约束平台公司不得传输给第三方,或另行存储、二次加工利用。

(2)健全关键领域国有公共数据资产开发利用政审制度

数据共享国有公共数据资产包括掌握在党、政、军以及有国资背景企事业单位的多源性大数据,此类数据资产应坚持“国家所有、统筹管理、充分利用、安全可控”的原则进行合理合规的开发利用[13]。特别是金融、生物基因等关键领域的国有公共数据,利用好了将利国利民、强国富民,野蛮生长轻则扰乱国民经济、社会秩序,重则祸国殃民、国家变色。例如,灰色资本方通过承接党政等方面的信息化项目,非法或过度收集国民个人隐私信息等数据,实现“千人千面”地精准营销、精准诈骗、精准推送不良游戏或信息,甚至帮助国外敌对资本以更低的成本践行“精神鸦片”“奶头乐”战略,最后造成社会发展缓慢,阶层分化、固化,影响我国共同富裕的历史进程。因此,为了加速推动国家治理体系和治理能力现代化,有必要按照现有的数据治理法律体系,健全关键领域国有公共数据资产开发利用政审制度。

(3)进一步推动“大国公器”数据安全运维的主动审计防御体系建设

如果金融、税务、公安大数据平台等“大国公器”被少数不法分子利用或掌控,可导致不法分子轻易解决“拜占庭将军”等类似的分布式共识问题,他们可以不经商议合谋,而高度一致地在金融、粮食等关键领域牟取巨利,或在税务、司法领域提前做出预判性对抗或逃避查办的动作。另外,数据共享信息系统首先是掌握在一线运维管理人员手里,然后数据或信息被逐级上报,最后由相关领导决策。其中的人员风险不可忽略,建议构建基于重点人群的多源数据监控法理机制和“民间举报+专家经验+机器智能”的主动防御体系。例如,平时应将运维人员纳入重点监控对象,签订保密协议,一旦发现异常行为或数据风险,可通过秘密的法理渠道,扩大行为审计监控范围,精准画像找内奸,清除立场不一致的“精英”,确保队伍的纯洁性。特别是对重大事件要及时发现和提前预见,并向相关业务平台和处置前端给出告警性提示乃至行动性指示,以便进行事前干预,改变以往深度依赖专业情报分析人员的被动式情报分析研判模式。

3.3 加强数字关键核心技术攻关和自主创新

随着中美贸易战及国际产业脱钩趋势等发展现状,我国想靠超大规模市场优势换取数字科技基础核心技术的老路已然不通,只有打好数字关键核心技术攻坚战,把数字经济自主权牢牢掌握在自己手中,才能引领数字经济发展,实现高水平自立自强。要充分发挥举国科技体制、网信重大工程、网信资源三大组织体系的优势,参考分级保护标准[14]和数据安全能力成熟度模型[15]等现有标准,加强数据脱敏、数字水印、隐私计算等数字关键核心技术攻关和自主创新,强化对 PKS 等自主计算产业体系支

www.pcachina.com

持力度，加快内生内置安全技术、可信计算3.0技术等方面的知识产权体系和标准规范体系建设，培养高层次人才，为未来可能面临的国家级大数据协同安全、核心技术动态对抗体系做准备。

3.4 分类分层制定数据资产管理战略规划

世界各国及我国内部不同区域、不同行业的信息化发展并不均衡，数据共享水平有高有低，发展阶段有快有慢。面对纷繁变化的数字环境和技术浪潮，为实现数据赋能行业、助力业务发展的目标，不同层级的政府机关、不同规模的企事业单位等均应结合上位数据治理法律体系和行业特性，体系化评估和摸底组织内部的数据资源现状、数据共享能力水平、数据合规以及数据安全发展相关需求，针对性地制定数据资产管理上层、中层和底层的战略规划，明确数据战略愿景和使命，梳理数据资产管理目标、路线、方法和措施，包括动静相宜、分类施策和分级定措等[6]数据规章流程和奖惩扶持等组织保障制度，为整个社会的数字化转型奠定基础。

4 结论

数据是数字经济发展的基础，数据共享是全社会、多领域数智化转型的基石，更是各国进行体系化竞争的关键。只有贯彻习近平总书记关于保障国家数据安全的理念，把“不断做强做优做大我国数字经济”当成面向未来数字经济发展的行动指南，才能让数字经济发挥重组全球要素资源、重塑全球经济结构、改变全球竞争格局的重要作用，构筑起国家发展竞争新优势[3]。

参考文献

[1] European Commission.A european strategy for data[EB/OL].(2020-02-19)[2021-10-26].https://ec.europa.eu/info/sites/default/files/communication-europeanstrategy-data-19feb2020_en.pdf.

[2] 宋卿清，曲婉，冯海红.国内外政府数据开发利用的进展及对我国的政策建议[J].中国科学院院刊，2020，35(6)：742-750.

[3] 习近平.不断做强做优做大我国数字经济[J].求是，2022(2)：4-8.

[4] 房殿军，郑卓远，洪晟，等.数据主权交换平台方案模式研究[J].信息技术与网络安全，2022，41(4)：2-10.

[5] 彭辉.数据权属的逻辑结构与赋权边界——基于“公地悲剧”和“反公地悲剧”的视角[J].比较法研究，2022(1)：101-115.

[6] 张雪莹，杨帅锋，王冲华，等.工业互联网数据安全分类分级防护框架研究[J].信息技术与网络安全，2021，40(1)：2-9.

[7] 夏义堃，管茜.政府数据资产管理的内涵、要素框架与运行模式[J].电子政务，2022(1)：2-13.

[8] 沈昌祥.用主动免疫可信计算3.0筑牢网络安全防线 营造清朗的网络空间[J].信息安全研究，2018，4(4)：282-302.

[9] GB17859-1999 计算机信息系统 安全保护等级划分准则[S].1999.

[10] 张会平，顾勤，徐忠波.政府数据授权运营的实现机制与内在机理研究——以成都市为例[J].电子政务，2021(5)：34-44.

[11] China Strategy Group.Asymmetric competition：a strategy for China & technology[R].2021.

[12] GB/T 37973-2019 信息安全技术——大数据安全管理指南[S].2019.

[13] 中国信息通信研究院云计算与大数据研究所.数据资产管理实践白皮书(3.0)[R/OL].[2021-09-18].https://max.book118.com/html/2018/1217/8077073-134001137.shtm.

[14] GB/T 22239-2019 信息安全技术——网络安全等级保护基本要求[S].2019.

[15] GB/T 37988-2019 信息安全技术——数据安全能力成熟度模型[S].2019.

(收稿日期：2022-06-07)

作者简介：

李建(1985-)，男，硕士，工程师，主要研究方向：信息系统架构设计、PKS体系标准化。

王昊(1983-)，男，硕士，高级工程师，主要研究方向：下一代网络架构与安全。

姜苏峰(1980-)，男，博士，讲师，主要研究方向：计算架构、系统工程。

www.pcachina.com

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