

数据共享交换平台全流程安全防护方法与技术研究

王 鹏¹, 王 亭², 张行宽²

- (1. 鄂尔多斯市东胜区大数据中心, 内蒙古 鄂尔多斯市 017000;
2. 内蒙古包钢钢联股份有限公司稀土钢冷轧板材厂, 内蒙古 包头 014010)

摘 要: 数据共享交换平台作为数字时代的重要产物, 既可突破信息壁垒, 也能够保障数据价值转化目标的实现。由于涵盖数据处理的多个环节, 包括采集、传输、存储和共享等, 因此该平台极大地支撑着跨部门、跨领域的协同。平台的开放化特征相对突出, 运行中面临的安全风险多种多样, 给平台安稳运行造成了影响。为维护平台的正常运行, 保障其功能的实现, 文章立足平台全流程的安全防护, 提出加强平台服务供应链管理、完善数据安全管理体系、强化防护技术应用等安全防护举措, 希望能够为平台运行筑牢安全防线, 维护数据流转各环节的安全性。

关键词: 数据共享交换平台; 安全风险; 全流程防护

中图分类号: TP393

文献标识码: B

文章编号: 1009-5438(2026)03-0092-04

Research on Full Process Safe Protection Methods and Technologies of Data Sharing and Exchange Platform

Wang Peng¹, Wang Ting², Zhang Xingkuan²

- (1. Ordos Dongsheng District Big Data Center, Ordos 017000, Inner Mongolia Autonomous Region, China;
2. Cold Rolled Rare Earth Steel Plate Plant of Inner Mongolia Baotou Steel Union Co., Ltd.,
Baotou 014010, Inner Mongolia Autonomous Region, China)

Abstract: The information barriers could be broken through and the target of data value conversion could be ensured to be realized with data sharing and exchange platform, important product of the digital age. Due to this platform covers several links of data processing including collection, transmission, storage and sharing, it greatly supports cross-department and cross-disciplinary collaborations. The open features of platform are relatively prominent and diverse security risks are faced in operations so that smooth operations of the platform are influenced. In order to maintain normal operations of the platform and ensure to realize its functions, such safe protection measures as strengthening the service supply chain management of platform, perfecting data security management system and strengthening applications of protection technologies are proposed based on full process safe protection of platform, which are hoped to strengthen the safety defense line for operations of platform to maintain the security in each link of data transmission, sharing and exchange.

Key words: data sharing and exchange platform; security risk; full process protection

全面数字化转型已成为当前社会发展的大势所趋,在此背景下,数据逐渐成为了核心的生产要素,这使得数据共享交换平台重要性逐步凸显。数据共享交换平台作为跨层级、跨区域数据互联互通的载体,既可以高效整合数据资源,也能便利数据资源后续的科学合理利用。然而,从现阶段平台的运行情况看,其效能的发挥中,也随之涌现了诸多的安全风险隐患,包括服务供应链建设漏洞、数据泄露和篡改、多节点多系统协同短板等,极大地威胁了数据的安全性,也影响着数据共享交换平台的稳定运行。故而,有必要探讨数据共享交换平台的全流程安防举措,这对于平台运行中安全风险的化解、数据交换共享的有序开展有重要的维护作用。

1 数据共享交换平台功能

一般而言,数据共享交换平台的架构大多为分层式(如图1),其中占据底层基础位置的是数据层,承担任务是对各业务系统多维度的数据汇集,要以统一数据标准为依据,保障清洗、整合与存储目标的良好实现,该层级在平台中属于数据的“蓄水池”。交换层属于平台的核心,其具备的能力是跨部门传输数据、协议转换等,该层级在数据的双向流转上主要是依靠安全传输通道,能为跨层级、跨系统的数据交换可信性、可控性提供保障^[1]。应用层面向广大用户群体开放,涉及功能包括数据查询、订阅等,可支撑政务协同、企业数据对接等诸多的业务场景,保障数据价值依靠实际的应用实现真正落地目标。

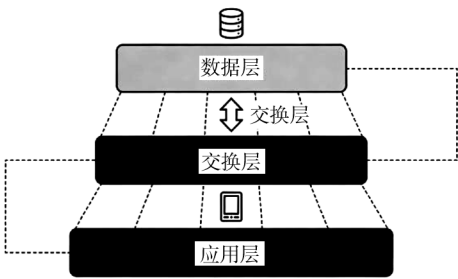


图1 平台架构参考图

立足于实际业务场景角度来看,平台的运行中数据汇聚和治理属于核心功能,通过与多元异构系统的对接,能够保障数据校验、去重等自动化完成,使数据孤岛问题得到良好解决^[2]。安全可控交换也属于平台极为重要的功能之一,其涉及加密传输、权限管控等环节,旨在为敏感数据跨部门、跨机构流

转中的全过程可追溯性提供保障。平台还具备数据服务功能,可在封装 API 接口、数据目录的基础上,保障业务系统对平台数据的按需调用。同时还支持可视化的监控,能通过对数据交换量、成功率指标等的实时和动态展示,助力运维人员对平台运行问题的高效化定位。

2 数据共享交换平台的安全风险

2.1 服务供应链建设风险

数据共享交换平台的运行与服务的提供就属于一个完整供应链,而这一供应链的基石就是信息通信技术和配套设施,其能够为社会各组织在平台上的操作营造物理环境^[3]。但需注意的是,由于信息通信技术、配套设施自身脆弱性、漏洞性因素的影响,或者是生产制造和研发方面存在不足,难免会存在一些信息安全风险。此种情况下,如何防范、控制供应链的安全风险,为平台服务、信息系统安全提供最大程度的保障作用,需平台运营主体加以关注。

2.2 数据、信息安全风险

受平台和网络开放性因素的影响,平台上的数据信息必然会面临诸多的安全风险。常见如下:①泄露,该风险来源于诸多环节,在平台与各主体对接的过程中,若未能加密传输链路、不够重视存储介质防护等,数据信息遭到非法截取或泄露的情况极易出现。②篡改,这种风险的的产生一般是因恶意攻击或操作失误所致,攻击者会依靠恶意代码注入、数据校验机制篡改等举措,破坏原有数据的真实性。③权限滥用,是因权限管控缺位所致,导致一些人员出现了越权访问的现象,进而形成了隐蔽安全漏洞,严重冲击平台数据信息安全,表1为多种风险类型和详细描述。

2.3 多节点多系统下的安全风险

由于平台内部的网络节点数量较多,加上涉及各种各样的信息系统,因此平台突出特征就是有诸多的网络节点、业务系统和数据资源。从常规且一般的安防举措看,包括防火墙、入侵防护系统等,通常侧重于保护网络边界,且对外部攻击的抵御通常是依靠流量分析、边界防护来实现,此类安防举措若面对的是 APT(高级可持续攻击),难免会出现力不从心的情况。APT 攻击流程见图2,其普遍特征就是针对性、隐蔽性较强,同时还存在高度复杂的情况,而攻击者采取此种攻击举措时,能够通过零日漏洞、社会工程学等手段,长期潜伏于系统之中,以达

到自身对系统数据的窃取目的。从平台接入的诸多业务系统看,其设计目的在于支撑业务协同、数据共享,这一过程在数据、业务的调用上通常是以开放

API 接口为载体,致使传输、共享数据中的泄露隐患大大增加。

表 1 多种风险类型与具体情况

风险类型	风险描述	潜在影响	典型场景
数据泄露	存储、传输中未授权访问或篡改	机密外泄、隐私曝光	跨部门交换
数据篡改	存储或传输时被恶意修改	决策依据失真,业务异常	供应链协同
权限滥用	内部人员越权访问非授权数据	违规数据、合规性违规	运维人员违规
数据残留	数据删除或迁移后仍有残留	被恶意恢复利用	存储空间清除
加密失效	加密算法强度不足或密钥管理漏洞	保护机制被迫且	使用弱加密算法

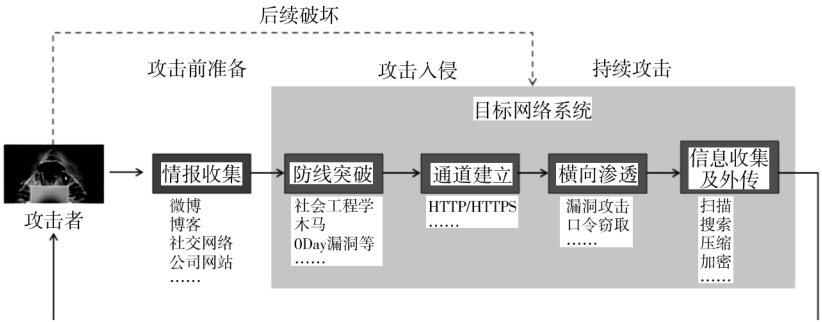


图 2 APT 攻击流程

3 数据共享交换平台全流程安全防护方法与技术

3.1 加强平台服务供应链管理

数据共享交换平台运行与服务提供作为一个完整的供应链,它的安全、可靠构建,离不开管理作用的发挥,本研究中加强平台服务供应链管理涉及的范畴主要包括设立技术标准、落实资质管理。现阶段,有必要侧重于系统化的角度,针对性构建自主可控的技术评估体系,使微处理器、操作系统等基础软硬件方面的可靠性瓶颈得到良好突破。①国家层面应健全技术标准规范,同时在研发投入上加大力度,并指引社会资本在关键技术攻关中的参与。②在供应商准入机制上严加把控,要落实多维度的审查工作,审查工作应聚焦资质认证、物理环境、安全制度等诸多层面,并将动态评估机制构建好。③加大对先进检测技术的利用,基于高水平、高能力的检测工作开展,使供应链漏洞得到及时发现和处理,确保平台脆弱性问题得到良好改善。

3.2 完善优化数据安全管理体系

数据交换共享平台的安全防范中,极为关键的一个举措就是健全对应的管理体系,其中重点考虑的就是完善组织架构,将数据管理的边界明确好。具体可采取以下措施:其一,科学分类、分级平台数据,以数据敏感度、重要性等为依据,就各个类别进行划分,以此为前提指导各类数据保护要求、安全级别的明确。其二,贯彻落实权限管理、访问控制,平台上数据的交换和共享中,遵循的一个必要原则应该是最小授权,其中要通过对诸多技术手段的应用,如身份认证、日志记录等,保障访问控制的严格落实,更多访问控制技术类型、功能、应用场景等见表 2。其三,进一步推进云平台的构建,以便在云平台上统一部署业务应用,构建覆盖数据全生命周期的纵深防御体系,确保形成标准化、体系化的安全防护能力。其四,在完善组织架构的基础上,从组织内部出发,构建数据全生命周期权责管理体系,明确各部门、各人员的管理职责、操作权限,确保数据全流程管理中安全责任的可视化与可追溯性。

表 2 访问控制关键技术应用

技术手段	核心功能	应用场景	实施效果
多因素认证	密码 + 生物特征 + 硬件令牌	高敏感数据访问	非法访问尝试降低 92%
属性基加密	基于用户属性的解密密码	跨部门数据共享	数据泄露事件减少 76%
区块链存证	操作记录不可篡改、全程可追溯	重要数据流转审计	审计效率提升 60%
动态权限管理	结合情境动态调整访问权限	临时数据协作场景	权限误用率下降 85%
行为分析引擎	机器学习识别异常访问模式	内部威胁检测	异常行为识别准确率达 93%

3.3 强化技术防护手段的应用

一方面,在平台网络安全上提高重视程度,具体要从信息系统的应用业务出发,以其安全需求、重要度为依据,立足多个维度落实信息安全等级保护举措,包括服务器、路由器和应用系统等,其中要注重对多种防护手段的综合应用,如防火墙、光闸等,加固主机的同时,有效防护病毒。同时,还可考虑对 SIEM、SOAR、XDR 等方案的部署,确保对威胁检测、响应的智能化目标得以良好实现。另一方面,基于密码式的信息认证手段,就可信可控交换技术进行应用,这方面要从实际场景出发,注重对多种隐私计算技术的整合利用,如同态加密、联邦学习等,确保隐私保护能够适配各层级、各重要性程度;或者是对区块链等技术的应用,促进数据流转中的高效追踪,使数据由源头至终端利用的全流程实现可视化管控目标。

这里聚焦“数据共享、交换”来分析技术防护手段的应用,数据共享强调协同性、而数据交换重在突出动态性,结合这方面特征,数据共享中相对适宜的技术手段有 ABE 技术(该技术应用示例见图 3),通过去中心化可信共享体系的构建,无需集中汇聚原本分散于各节点的原始数据,仅依靠密钥分级管理机制,就能立足不同权限主体,科学且合理分配差异化的访问密钥,这既为多主体协同化、便捷化共享提供了保障,也能有效防范数据泄露的风险。对于数据交换,建议以可信交换网关技术为载体,通过专用交换通道的搭建,双向校验进出交换节点的数据,这一过程在进行预处理操作的情况下,如数据脱敏、格式标准化转换等,可有效消除其中的敏感冗余信息,为交换过程的合规性提供保障;与此同时,基于区块链存证技术的科学部署,将数据交互全要素写入分布式账本,能确保数据交换全流程的可追溯性且不可篡改^[9]。

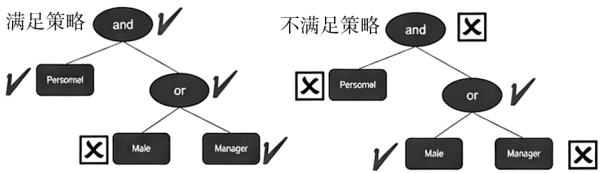


图 3 ABE 应用示例

4 结束语

数据共享交换平台是否始终处于安全、稳定运行状态,与平台效能发挥情况息息相关。该平台的安防工作具备较强系统性,也需持续推进,更应该在平台运行的全流程深入贯彻。为实现最大化的安防目标,文章在深层次剖析平台安全风险的基础上,从供应链管理、安全体系建设、技术防护等角度出发提出了具体的安防举措,指导平台对运行中安全风险的防控。随着数字化、信息化技术的进一步迭代,加之安全风险的不断演变,平台安防中也要落实动态的优化和调整,以指导安防策略的针对性改进,为平台安全、高效运行提供长效保护,最大程度释放平台的数据价值。

参 考 文 献

[1] 任伟峰. 内网敏感大数据共享交换安全性监控平台设计[J]. 信息技术, 2022, 46(10): 118-123.

[2] 张丹, 李云杰, 孟宪军, 等. 智慧校园数据共享与交换平台建设[J]. 深圳职业技术学院学报, 2022, 21(5): 16-21.

[3] 廖淑珍, 吴易轩, 石雨潭, 等. 基于事件溯源的数据共享交换平台的设计[J]. 广西开放大学学报, 2024, 35(1): 28-32.