



电力大数据安全治理体系研究

朱洪斌¹, 安龙², 杨铭辰³

- (1. 国家电网有限公司大数据中心, 北京 100031;
2. 国网山西省电力公司信息通信分公司, 山西 太原 030021;
3. 国网陕西省电力公司西咸新区供电公司, 陕西 西咸新区 712000)

摘要: 近年来, 针对大数据的勒索攻击事件和数据泄露问题日趋严重, 针对数据安全国家相继出台了一系列相关法律法规, 明确了大数据安全工作的要求, 电力大数据资产具有数据量大、分布面广、利用价值高、敏感度高等特点, 急需开展大数据安全治理技术研究。在分析电力大数据安全面临的挑战的基础上, 设计了电力大数据安全治理体系, 提出了电力大数据安全治理要求, 研发了电力大数据安全治理平台, 在实验中对数据安全管控进行了验证。

关键词: 电力大数据; 数据安全; 安全管理; 治理体系

中图分类号: TM715

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019281

Research and practice on power big data security governance system

ZHU Hongbin¹, AN Long², YANG Mingchen³

1. Big Data Center of State Grid Corporation Of China, Beijing 100031, China
2. State Grid Shanxi Electric Power Company Information and Communication Branch, Taiyuan 030021, China
3. State Grid Shaanxi Electric Power Company Xixian New Area Power Supply Company, Xixian New Area, Shaanxi 712000, China

Abstract: The blackmail attacks and data leakage problems of big data had become increasingly serious in recent years, and the state had successively issued a series of relevant laws and regulations to clarify the requirements for big data security work. Power big data assets had the characteristics of large data volume, wide distribution, high utilization value and high sensitivity. It was urgent to carry out research on big data security governance technology. Based on the analysis of the challenges faced by power big data security, the power big data security governance system was designed, the power big data security governance requirements were put forward, and the data security management and control was verified by the research and development of power big data security governance platform.

Key words: power big data, data security, security management, governance system

1 引言

随着泛在电力物联网^[1]的发展,国家电网公司大力拓展数字经济市场,并建设国网大数据中心(以下简称大数据中心)作为未来海量数据的集中分析、处理、共享、运营的重要环节。大数据中心定位于国家电网公司数据管理专业机构和数据融合平台、服务平台、应用支撑平台,数据资产具有数据量大、分布面广、利用价值高、敏感度高等特点。

近年来,针对大数据的勒索攻击事件^[2]和数据泄露问题日趋严重,地下数据交易黑色、灰色产业也导致了大量的数据滥用和网络诈骗事件。为确保大数据中心的安全稳定运行,有必要开展大数据中心安全治理技术研究,在现有安全要求的基础上,规划设计完整的数据安全治理体系^[3-4],保障大数据中心业务和数据安全。

针对数据安全,国家已相继出台了一系列相关法律法规要求:2016年12月,国家互联网信息办公室发布了《国家网络空间安全战略》,提出实施国家大数据战略,建立大数据安全管理制度,支持大数据信息技术创新和应用要求;2017年6月起实施的《中华人民共和国网络安全法》提出,鼓励开发网络数据安全保护和利用技术;全国人民代表大会常务委员会和工业和信息化部、公安部等部门为加快构建大数据安全保障体系,相继出台了《加强网络信息保护的決定》《电信和互联网用户个人信息保护规定》等一系列法规和部门规章制度,为大数据安全工作的开展提供了指导和依据。

2 电力大数据面临的安全挑战

大数据的一个显著特点是数量巨大且相互关联,其中蕴含着巨大的价值。伴随着电力物联网中电力大数据的集中处理、广泛共享、交叉使用,电力大数据安全问题^[5-6]日益凸显,数据安全面临着严峻挑战。

2.1 复杂开放环境下数据防护难度加大

电力大数据业务环境将更加开放,业务生态将更加复杂,参与数据处理的角色将更多元,系统、业务、组织的边界将进一步模糊,导致数据的产生、流动、处理等过程比以往更加丰富和多样,使得大数据在保密性、完整性、可用性等方面面临着更大的挑战。

数据开放共享以及频繁流动使得防范更加困难。大数据应用体系庞杂,频繁的数据共享和交换促使数据流动路径变得交错复杂,数据从产生到销毁不再是单向、单路径的简单流动模式,也不再仅限于组织内部流转,而会从一个数据控制者流向另一个控制者。在此过程中,实现复杂交换路径下的追踪溯源将更加困难,特别是数据标记的可信性、数据标记与内容之间关联的安全性等问题更加突出。

2.2 个人信息泄露风险加剧

电力大数据应用对个人隐私造成的危害不仅是数据泄露,大数据采集、处理、分析数据的方式和能力对传统个人隐私保护框架和技术能力亦带来了严峻挑战。随着数据挖掘、机器学习、人工智能等技术的研究和应用,大数据分析的能力越来越强大,从碎片化的、不具有敏感性的数据中可以分析出更多的个人信息,海量数据的聚合甚至可以分析出涉及企业核心利益以及国家安全的信息。大数据时代,要对数据进行安全保护,既要注意防止因数据丢失而直接导致的个人信息泄露,也要注意防止因挖掘分析而间接导致的个人信息泄露,这种综合保护需求带来的安全挑战是巨大的。

2.3 传统安全措施难以适配大数据应用场景

电力大数据应用多基于开放的分布式计算和存储架构为其提供海量数据分布式存储和高效计算服务,这些技术和架构使得大数据应用的系统边界变得模糊,数据可能动态分散在很多个不同的存储设备,甚至不同的物理地点中存储,这样导致难以准确划定传统意义上的每个数据集的“边界”,传统



基于边界的安全保护措施将变得不再有效。

传统数据访问控制技术无法解决跨组织的数据授权管理和数据流向追踪问题，仅依靠协议难以实现对数据接收方的数据处理活动进行实时监控和审计，极易造成数据滥用的风险。

传统的安全检测技术能够将大量的日志数据集中到一起，进行整体性的安全分析，试图从中发现安全事件。然而，这些安全检测技术往往存在误报过多的问题，随着大数据系统的建设，日志数据规模增大，数据的种类将更加丰富。过多的误判会造成安全检测系统失效，降低安全检测能力。

3 电力大数据安全治理体系设计

为促进数据安全合规使用，保障业务安全稳定运行，本文依据国家数据安全相关法律法规要求，以数据安全为核心，设计了电力大数据安全治理体系，如图1所示，全面提升数据全生命周期安全保障能力，推进数据安全攻防、检测、评估、监测等技术的研究应用，对内对外提供数据安全服务。

电力大数据安全治理体系包括安全管理^[7]、基础设施安全^[8]、数据与个人信息保护^[9]、数据安全运营及服务和技术支撑等内容。

3.1 安全管理

安全管理重点遵循国家法律法规关于数据及

个人信息保护的要求，建立大数据中心安全管理体系，落实责任，包括组织机构、制度建设、合规管控、应急响应和技术标准等。

3.2 基础设施安全

基础设施安全包括大数据中心的物理、网络、主机和云环境的安全防护以及大数据平台的安全防护。按照等级保护及公司顶层设计总体技术要求落实相关防护措施。

3.3 数据安全及个人信息保护

数据安全及个人信息保护重点开展数据全生命周期安全防护，建立覆盖数据和个人信息全环节的安全防护措施，综合利用数据源验证、传输加密、隐私保护、数据交易安全、数据防泄露、追踪溯源、数据销毁等技术，与现有网络安全技术相结合，有效地提升数据全生命周期安全防护能力。

3.4 数据安全运营及服务

数据安全运营及服务重点依托大数据中心的海量数据资源，利用大数据、人工智能等综合分析功能，提升大数据中心网络安全智能防御能力，同时形成业务风险预警、安全态势感知、内外部情报分析和舆情监测等核心能力，对内对外提供安全服务。

3.5 技术支撑

为保障大数据中心安全，从安全评估、安全

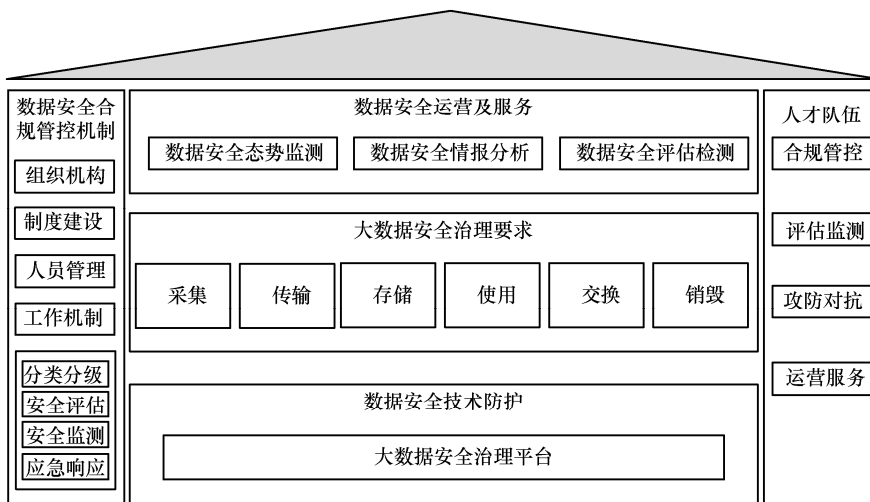


图1 电力大数据安全治理体系

攻防、实验检测、技术研究等方面开展数据安全技术支持工作，确保数据安全防护切实有效。

4 电力大数据安全治理要求

4.1 数据收集

数据收集时，应遵循合法、正当、必要的原则，公开收集使用规则，明示收集信息的目的、方式和范围，并经过被收集者同意。收集时采取必要的安全技术手段和管控措施，对收集到数据进行完整性和一致性校验，跟踪记录数据收集获取的过程，确保数据收集过程的可追溯性。

4.2 数据传输

数据内部传输和外部传输应采用不同的加密、签名、鉴别、认证等机制对传输中的数据进行安全管理，防止传输过程中的数据泄露^[10]。建立传输通道前，对传输两端的主体身份进行鉴别和认证，确保数据传输双方是可信任的。

4.3 数据存储

严格按照国家数据安全要求，加强大数据中心内部数据存储安全保护^[11]。采取认证鉴权、访问控制、加密、安全审计等安全措施，做好数据存储保护。依据数据级别做好数据备份策略，确保备份与恢复功能，保证数据的高可用性和灾难可恢复性。

4.4 数据处理

利用核心业务支撑平台实现数据的统一分析处理，对外不提供明细数据，仅提供经脱敏或加工后的数据，防止敏感数据泄露。加强对重要数据使用行为的识别、监控和预警，并签订相应安全职责及保密协议。

4.5 数据交换

针对数据导入导出，结合业务需求和数据分级明确数据导入导出策略与规范，严格安全评估及授权审批流程。针对数据共享，明确数据共享范围和安全管控措施。针对数据发布，依据国家法律法规建立数据发布审核制度，各专业自行明

确数据发布的内容、范围、规范以及发布者与使用者的权利和义务。

4.6 数据销毁

明确数据销毁工作责任，制定数据销毁策略和管理制度。根据数据安全分级和场景需要，确定数据销毁手段和方法，确保销毁数据不可复原。

4.7 安全事件处置

制定数据安全事件应急预案，明确各岗位职责及应急处置策略和流程，确保发生安全事件能及时响应并开展处置工作，记录事件内容，评估事件影响。

5 电力大数据安全治理平台研发和实践

5.1 电力大数据安全治理平台研发

电力大数据安全治理平台通过数据权限统一管控、安全策略集中管理、基于虚拟数据库的数据安全分发、灵活的数据防护能力以及数据使用过程中的安全监控等措施，实现大数据中心对外提供数据服务过程中的涵盖数据采集、传输、存储、使用、交换、销毁等全过程的安全管控。

电力大数据安全治理平台主要分为 4 层：数据交互层、数据服务层、数据存储层和数据接口层，如图 2 所示。

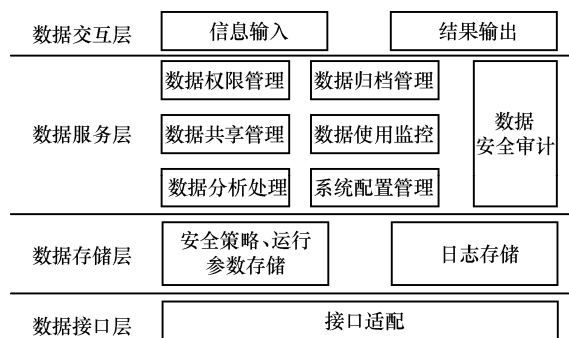


图 2 电力大数据安全治理平台

数据交互层负责接收用户或者应用的输入，并将输出通过各功能或者结果返回给用户或者应用；数据服务层负责数据申请、脱敏、使用、回收等数据全生命周期的管理，将数据从下发到回



收形成一个端到端的闭环管理；数据存储层负责将数据系统的用户信息、权限信息、敏感信息、使用信息、监控信息以及系统运行日志等存储到数据库；数据接口层负责与数据源之间的交互。

5.2 电力大数据安全治理平台实践验证

为了验证所提方法的有效性，搭建了大数据安全治理平台仿真环境，如图3所示。

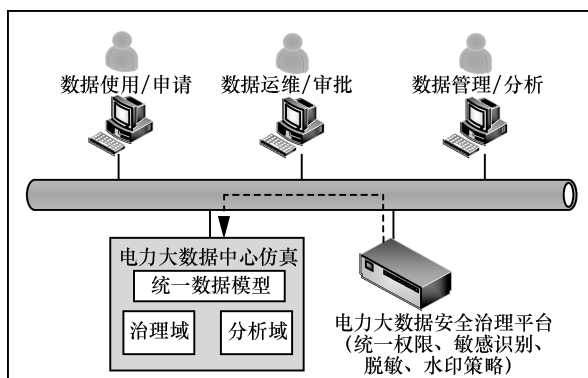


图3 电力大数据安全治理平台仿真环境

在上述仿真环境中，采用电力大数据安全治理平台对中心内部数据使用申请场景进行了实践验证，如图4所示。

在实践验证中，通过电力大数据安全治理平台，进行如下操作：数据申请人员在使用大数据中心仿真环境统一服务目录所提供的数据服务之前，首先向大数据安全治理平台提交数据使用申请，说明需要使用哪些数据以及申请数据的用途；通过审批后，由大数据安全治理平台后台进行数据抽取、敏感数据脱敏、水印标记添加、数据使用权限配置，其后将数据共享给申请人员；数据申请人员在使用大数据中心仿真环境共享的数据时，大数据安全治理平台也将同步监视用户数据使用行为；申请人员对数据使用完毕后，大数据安全治理平台进行数据归档和数据销毁。

为了方便实验，实验场景设计为：选取16 GB业务数据存储于数据库中，数据使用者向平台申请10 GB数据，其中包含敏感数据5 GB；数据使用者分别进行权限内/权限外数据访问。

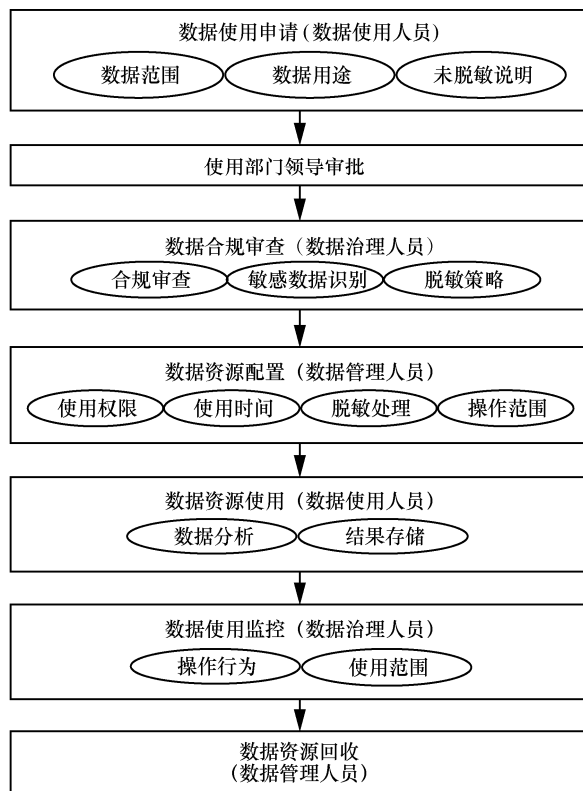


图4 内部数据使用申请场景管控设计

在实验中，电力大数据安全治理平台接收到数据使用申请，对使用者数据资源进行了权限确认、敏感识别和结果归档管理。实验结果显示：平台对使用者权限内数据的访问行为进行了数据资源配置，数据静态脱敏能力达到每小时8 Gbit，对使用者权限外数据访问的越权访问行为进行了有效识别和拒绝。

通过对典型应用场景的实践验证表明，电力大数据安全治理平台针对大数据的数据分析、处理等场景，能够自动高效地完成数据安全的管控，确保数据存储、共享、分析、使用、回收各环节的数据安全。

6 结束语

随着泛在电力物联网的建设，数据的共享和流通将更加频繁，电力大数据安全问题也日益凸显，数据安全面临着严峻挑战。

本文通过分析电力大数据^[12]面临的安全挑

战,设计了电力大数据安全治理体系,通过研发电力大数据安全治理平台对电力大数据安全治理管控进行了实践验证,通过验证表明,电力大数据安全治理平台有效地健全了数据安全管控机制,构建了数据安全合规技术支撑和安全运营服务能力,稳步提升了大数据中心整体数据安全管控能力。

参考文献:

- [1] 曾鸣,王雨晴,李明珠,等. 泛在电力物联网体系架构及实施方案初探[J]. 智慧电力, 2019, 47(4): 1-7, 58.
ZENG M, WANG Y Q, LI M Z, et al. Preliminary study on the architecture and implementation plan of widespread power internet of things[J]. Smart Power, 2019, 47(4): 1-7, 58.
- [2] 赵佩. 勒索病毒攻击事件漏洞分析及应对防护策略[J]. 电子技术与软件工程, 2019(4): 201.
ZHAO P. Vulnerability analysis and response protection strategy of Ransom ware attack event[J]. Network Security Technology & Application, 2019(4): 201.
- [3] 吴信东,董丙冰,堵新政,等. 数据治理技术[J]. 软件学报, 2019, 30(9): 25-27.
WU X D, DONG B B, DU X Z, et al. Data governance technology [J]. Journal of Software, 2019, 30(9): 25-27.
- [4] 史琳,吴疆,吴霞虹. 电力企业级数据治理体系的研究[J]. 电子世界, 2018(22): 184-185.
SHI L, WU J, WU X H. Research on power enterprise data management system [J]. Electronics World, 2018(22): 184-185.
- [5] 韩昌选,乐璐. 大数据时代下信息数据安全的探讨[J]. 电子技术与软件工程, 2013(24): 227-228.
HAN C X, LE L. Discussion on the security of information data in the age of big data [J]. Electronic Technology & Software Engineering, 2013(24): 227-228.
- [6] 周景. 大数据时代信息安全的防范对策思考与探讨[J]. 信息与电脑, 2019(2): 218-220.
ZHOU J. Thinking and discussion on the countermeasures of information security in the age of big data [J]. Computer Programming Skills & Maintenance, 2019(2): 218-220.
- [7] 秦体德. 浅析计算机网络安全管理技术的开发及应用[J]. 湖北科技学院学报, 2013(10): 19-20.
QIN T D. Analysis on the development and application of computer network security management technology[J]. Journal of Hubei University of Science and Technology, 2013(10): 19-20.
- [8] 沈玲. 美国如何保护关键信息基础设施[N]. 人民邮电, 2016-11-30 (6).
SHEN L. How the United States protects critical information infrastructure[N]. People's post and telecommunications, 2016-11-30 (6).
- [9] 张新刚,于波,程新党,等. 大数据与云计算环境下个人信息安全协同保护研究[J]. 电脑知识与技术, 2016(3): 53-55.
ZHANG X G, YU B, CHENG X D, et al. Research on collaborative protection of personal information security in big data and cloud computing environment [J]. Computer Knowledge and Technology, 2016(3): 53-55.
- [10] 童云海,陶有东,唐世渭,等. 隐私保护数据发布中身份保持的匿名方法[J]. 软件学报, 2010(4): 771-781.
TONG Y H, TAO Y D, TANG S W, et al. Identity-reserved anonymity in privacy preserving data publishing [J]. Journal of Software, 2010(4): 771-781.
- [11] 张亮. 基于云计算环境的大数据安全存储机制研究[D]. 南京:东南大学, 2016.
ZHANG L. Research on secure storage mechanisms for big data based on cloud computing [D]. Nanjing: Southeast University, 2016.
- [12] 李如初,沈名龙,彭海棠. 大数据、云计算在电力工业中的应用[J]. 电信科学, 2018, 34(4): 151-155.
LI R C, SHEN M L, PENG H T. Application of big data and cloud computing in power industry[J]. Telecommunications Science, 2018, 34(4): 151-155.

[作者简介]



朱洪斌(1980—),男,国家电网有限公司大数据中心高级工程师,主要研究方向为数据安全、安全运行等。



安龙(1988—),男,国网山西省电力公司信息通信分公司工程师,主要研究方向为信息安全、数据安全等。



杨铭辰(1986—),男,国网陕西省电力公司西咸新区供电公司工程师,主要研究方向为数据管理、信息安全等。