大数据安全特征与运营实践

刘志勇，何忠江，阮宜龙，单俊峰，张超
（中国电信集团有限公司，北京 100032）

摘　要：随着数据类型、用户角色和应用需求的不断细化，以及大数据复杂的数据存储和流动场景的出现，大数据安全防护要求越来越高。以大数据安全特征和运营实践为切入点，分析了大数据安全特征和技术发展趋势，体系化地梳理和总结中国电信以“数据和人”为核心的大数据安全深度防御体系建设和运营实践；并对区块链、联邦学习、人工智能、零信任等新技术在数据安全流通、数据安全风险监测、数据访问控制的引入提出了思考和展望。分析了大数据安全特征和技术发展的趋势，梳理了中国电信在大数据安全方面的运营实践，对新形势下筑牢大数据安全提出了思考与建议。

关键词：大数据；数据安全；区块链；联邦学习；人工智能；云计算
中图分类号：TP311
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021102

Big data security features and operation practices

LIU Zhiyong, HE Zhongjiang, RUAN Yilong, SHAN Junfeng, ZHANG Chao
China Telecom Group Co., Ltd., Beijing 100032, China

Abstract: With the continuous refinement of data types, user roles and application requirements, as well as the complex data storage and flow scenarios of big data, the requirement of big data security is higher and higher. Starting from the security characteristics and operation practice of big data, the security characteristics and technology development trend of big data were analyzed, the construction and operation practice of China Telecom’s big data security defense system with “data and people” as the core was systematically summarized. Some thoughts and prospects for the introduction of new technologies were also raised such as blockchain, federated learning, artificial intelligence and zero trust in data security circulation, data security risk monitoring and data access control.

Key words: big data, data security, blockchain, federated learning, artificial intelligence, cloud computing

1　引言

大数据已经逐步应用于产业发展、政府治理、民生改善等领域，大幅度提高了人们的生产效率和生活水平。适应、把握、引领大数据，将成为时代潮流。在大数据时代，数据是重要的战略资源，是企业得以发展的核心，但数据资源的价值只有在流通和应用过程中才能够充分体现。云计算、物联网、大数据等新技术的迅猛发展，引发了数据规模的爆炸式增长和数据模式的高度复杂化，如何对大量且复杂的数据进行有效管理和合理分析成为企业亟待解决的问题[1]。为应对日益

收稿日期：2021−04−10；修回日期：2020−05−15

复杂的数据环境，加快数据应用与部署，大数据湖逐渐成为企业大数据运营管理的重要趋势和发展方向，通过统一汇聚和管理各生产系统的运营数据，提供统一的存储与数据服务，让各类数据应用和数据开发人员各取所需，充分发挥数据价值[2]。大数据在收集、汇聚、存储、使用、共享的过程中，对信息安全的要求越来越高，数据类型及数据量的增多使数据安全和隐私保护问题更加突出，传统的基于边界安全和基于已知特征的网络安全防护方式，已无法有效应对大数据环境下新的安全威胁。因此，要建立完备的大数据安全防护机制和管理制度，根据各类数据应用的不同特点，完善全生命周期数据安全保障策略，防止数据越权访问、私自篡改、泄露毁坏等问题发生。

2　大数据安全特征和发展趋势

2.1　大数据安全特征

大数据（big data）具有数据体量浩大（volume）、数据生成速度快（velocity）、数据种类繁多（variety）、数据价值高但密度低（value）的 4V 特点，如图 1 所示。

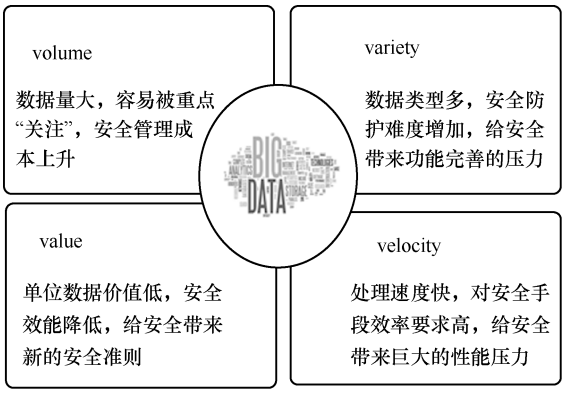

图 1　大数据 4V 特点

由于采用分布式存储方式，数据存储路径相对清晰，且数据量过大，导致攻击者较容易利用相关漏洞实施不法操作，造成安全问题。

（1）大数据成为网络攻击的显著目标。更加庞大敏感的数据提高了黑客的“收益率”，成为了黑客攻击的最佳目标；数据中包含大量用户信息，使得对大数据的开发利用很容易侵犯公民的隐私，增加了用户个人隐私泄露风险。

（2）大数据的存储管理风险加大。数据量非线性甚至指数级的速度增长，多种应用进程的并发以及频繁无序的运行，极易造成数据存储错位和数据管理混乱；访问控制和隐私管理、授权与验证的安全模式、技术漏洞和成熟度、数据管理与保密等问题，以及物理故障、人为误操作、软件故障、木马病毒和黑客攻击等都严重威胁着数据的安全性。

（3）大数据的传输处理隐患增多。除数据非授权使用、泄露、被篡改、被破坏等风险外，由于大数据传输的异构、多源、关联等特点，即使多个数据集各自脱敏处理，数据集仍然存在关联分析造成个人信息泄露的风险。

（4）大数据实施访问控制更加复杂。大数据应用范围广泛，被用于多种不同场景，被来自不同组织、部门、身份与目的的用户所访问，其访问控制需求十分突出，导致难以预设角色、难以实现角色划分、难以预知每个角色的实际权限、不同类型的大数据中可能存在多样化的访问控制需求等问题。

（5）大数据技术被应用到攻击手段中。网络攻击者最大限度地收集更多有用信息，通过大数据分析让攻击更加精准；大数据已成为高级可持续攻击（advanced persistent threat，APT）的载体，利用大数据发起僵尸网络攻击，控制上百万台傀儡机，传统的基于内置攻击事件库的特征实施匹配检测技术对检测 APT 攻击是无效的，将攻击隐藏在大数据中，给安全服务提供商的安全分析制造了很大的困难[3]。

2.2　大数据安全发展趋势

（1）数字化

面向云网安全协同和安全融云，建设“全网联动、防控一体”安全中台枢纽，打造以数据驱

动的智能化安全运营体系，从被动防御向积极防御演进。随着 IT 系统上云同步建立电信云内生安全体系，保障云上系统与数据安全，借助基础网优势，持续优化企业网络安全建设；并进一步打造以骨干网、5G 为中心的安全防护体系；构建 5G 核心网异常信令监测控制能力，打造差异化的 5G 安全防护体系，助力企业在 5G 时代提升整体竞争力；同时，逐步加强边缘网络安全防护能力，构建从终端到业务的零信任安全体系。重点攻关数据流动的阻断防护和安全检测技术，掌握敏感数据的识别、用户身份识别和访问控制、用户行为分析、个人隐私保护、数据防泄露等关键技术，实现安全能力服务化，统一开放和安全原子能力赋能数字化平台。

（2）体系化

构建贯穿大数据应用云管端的综合立体防御体系，已满足大数据战略与市场应用的需要。综合利用数据源验证、大规模传输加密、非关系型数据库加密存储、数据防泄露、数据销毁等技术，与系统现有网络信息安全技术设施相结合，建立纵深的防御体系。集中的安全配置管理和安全机制部署成为平台层安全趋势。集中安全管理、准入控制、多因素认证、细粒度访问控制、密钥管理、数据脱敏、集中审计等安全机制，从机制上防止数据的未授权访问和泄露。

（3）智能化

敏感数据识别技术作为数据安全监控的必要技术条件将逐步实现自动化；人工智能识别技术的引入，通过机器学习实现大量文档的聚类分析，自动生成分类规则库，内容自动化识别程度正逐步提高。大数据分析技术、机器学习算法的发展与演进将推动数据防泄露的智能化发展，DLP 将实现用户行为分析与数据内容的智能识别，实现数据的智能化分层、分级保护，并提供终端、网络、云端协同一体的敏感数据动态集中管控体系。借助大数据分析、人工智能等技术，实现自动化威胁识别、风险阻断和攻击溯源，从源头上提升大数据安全防御水平[4]。

（4）流通化

大数据要发挥其自身价值，必须安全、有效地流通、共享。之前应用广泛的数据脱敏技术受到多源数据汇聚的严重挑战而可能面临失效，目前匿名化算法等前沿技术鲜有实际应用案例，普遍存在运算效率过低、开销过大等问题，还需要在算法的优化方面持续进行改进，以满足大数据环境下的隐私保护需求。“隐私保护计算”和“区块链”成为近年数据安全流通领域常用的两种技术框架，通常涵盖联邦学习、安全多方计算、同态加密等关键技术。

3 大数据安全运营实践

目前，中国电信通过建设集团企业级大数据平台汇聚企业主要运营数据，开展精准营销、精确管理、精细服务、精益运营等应用探索，对部分生产系统闭环注智，较好地支撑了企业数字化转型。为解决大数据平台在数据汇聚和应用过程中的数据安全问题，打造了以网络基础设施安全为基础，以“数据和人”为核心的大数据安全深度防御体系，如图 2 所示，结合不同场景，从数据的采集安全、存储加工安全、应用共享安全等全生命周期进行综合施策，以此实现“降低数据泄露风险、保障企业级数据与用户隐私数据安全、夯实数字化基础”的目标。

3.1 夯实网络基础设施安全

网络基础设施安全是大数据安全不可或缺的基础保障。为满足“云网融合”安全需求，正在推动构建覆盖“云–网–应用–数据–终端”的一体化安全运营体系，从被动响应转向主动防御，从单点防御转向全网联防联动，建立安全与信息化“深度融合、全面覆盖”的内生安全体系，保障云网业务数据安全、可靠、高效地运营。在网络安全层面，大数据平台实施物理隔离部署，日常管

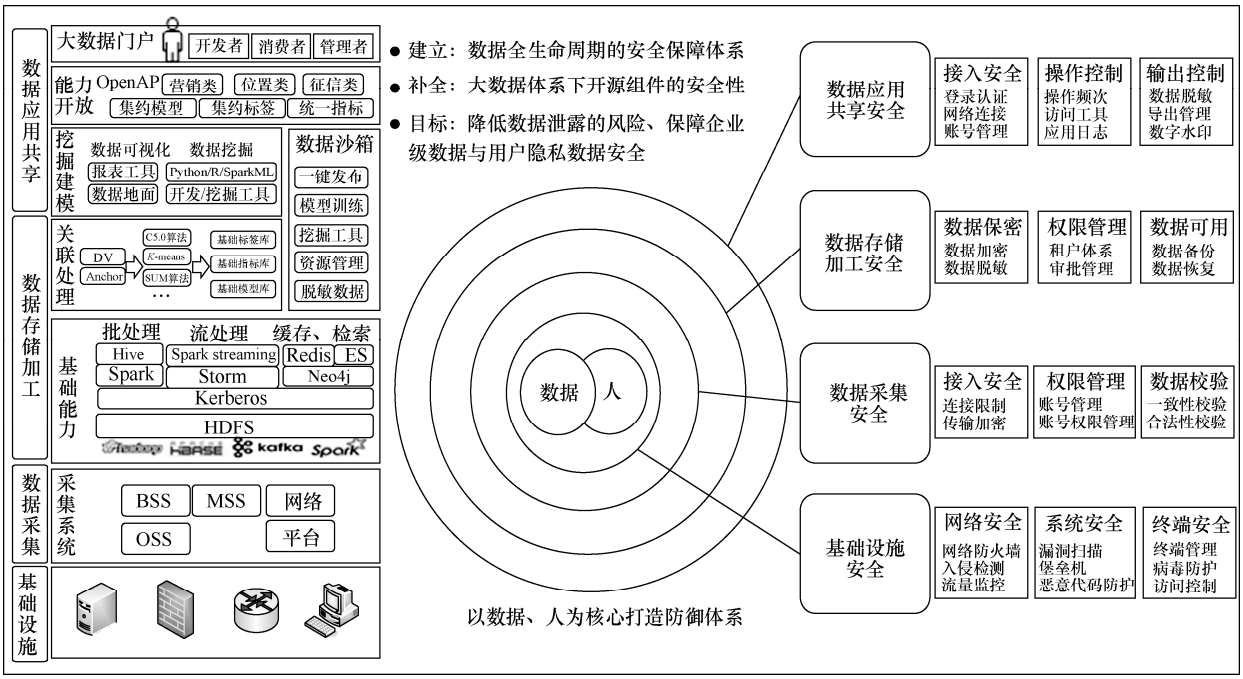

图 2　打造以数据、人为核心的大数据安全防御体系

理维护、开发测试均通过“VPN+堡垒机”方式接入；网络边界出口部署流量控制、入侵检测系统（intrusion detection system，IDS）、入侵防御（软 WAF）等安全防护设备，通过策略路由方式引流，防范南北向攻击；利用云堤网络链路资源和基础清洗能力，结合网站防护设备（硬 WAF），实现基于 IP 路由的双向引流、清洗和综合防护，防止大流量 DDoS 攻击、Web 攻击；使用 WAF+SSL 证书进行应用层、传输层的防护，保证数据不被劫持、篡改，防止 CC、SQL 注入等攻击。在主机安全层面，采用 LDAP 统一身份认证和主机权限控制；部署安全代理（agent）监控组件对主机实现 7×24 h 的安全防护，部署终端防护响应工具（EDR），通过预防、防御、检测、响应等环节，为终端提供更加优良的隔离策略、病毒查杀和检测处置能力。

3.2　完善大数据安全技术体系

围绕数据全生命周期，从采集、传输、存储、处理、共享、销毁等环节，以关键技术措施为突破，完善大数据安全技术体系，如图 3 所示。

（1）在数据采集环节，实施连接限制、敏感数据识别、数据一致性和合法性校验等手段，通过底层 HDFS 文件系统的访问控制列表（access control list，ACL）权限管控实现数据源认证、接入安全、权限管理；开启基于分析系统日志（Elastic search，Logstash，Kibana，ELK）开发的数据采集日志审计，实现对数据采集过程全流程操作可追溯，保证各类数据采集活动的合规性和安全性；对采集的数据进行分类分级标识，对不同类和级别的数据实施相应的安全管理策略和保障措施[5]。

（2）在数据传输环节，利用链路加密、加密协议、认证鉴权等机制对数据传输进行安全管理，构建传输安全通道；部署 RSA、AES 等密码算法以及 PKI 系统进行身份认证和密钥管理，防止数据丢失、泄露、篡改。建立数据传输接口安全管理工作规范，包括安全域内、安全域间等数据传输接口规范。

（3）在数据存储与加工环节，采用多种加密算法（例如 AES、FPR）实现数据脱敏、加密等

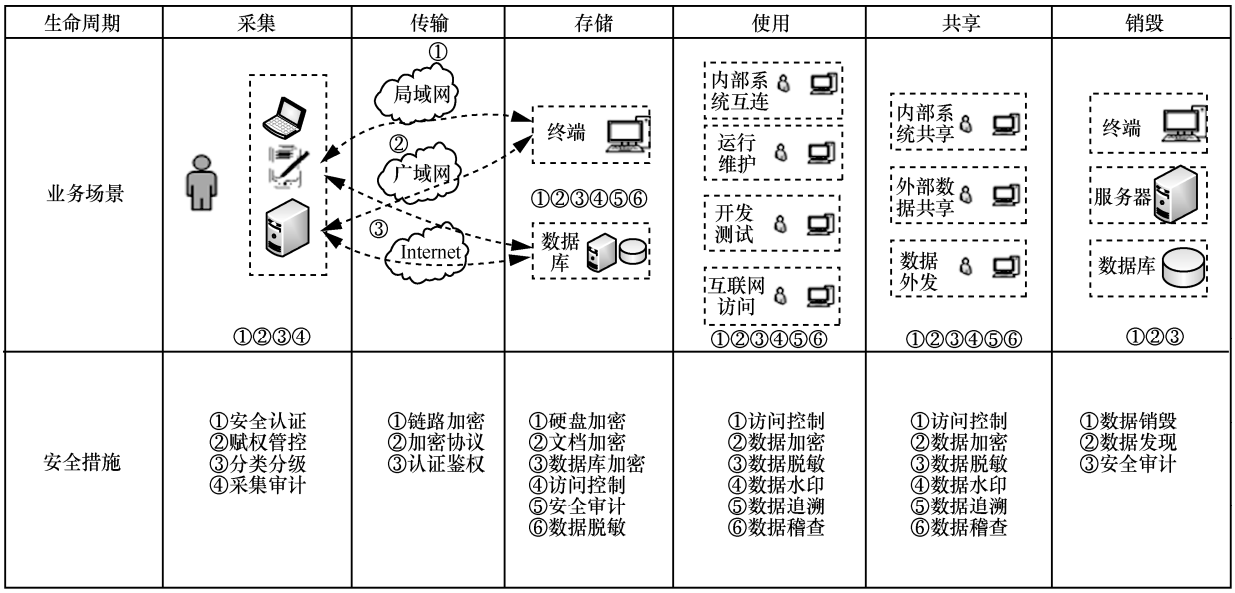

图 3　数据全生命周期安全管理

手段。实现数据保密，提高个人信息的安全性；加强数据的统一调度与资源监控，以及日志分析和操作审计；对数据实施分权分域管理，严控集群公共数据的读写权限分配，数据模型采用分层架构，控制数据开放范围。

（4）在数据应用与共享环节，实施数据脱敏、数据水印、导出管理、访问频度控制等手段，建立严格的审批流程，通过访问控制列表（ACL）、业务日志监控（sentry）等技术实现对数据、表的共享访问控制和操作控制。制定数据共享审计策略和审计日志管理规范，审计记录详细完整，为数据共享安全事件的处置、应急响应和事后溯源提供帮助[6]。

（5）在数据销毁层面，针对不同的存储方式、存储内容，建立数据销毁周期管理能力，明确需要进行数据销毁的数据、方式和要求，明确销毁数据范围和流程；遵循可审计原则，建立数据删除策略和管理制度，记录数据删除的操作时间、操作人、操作方式、数据内容等相关信息[5]。

3.3　大数据安全实践

着眼云网融合资源布局的多组织、大体系环境下的数据安全需求，建设企业级大数据平台安全管理系统，构建大数据集群安全统一管控体系，通过数据分权分域管理、数据访问授权、数据加密脱敏、敏感数据识别、安全审计实时风险告警、集群多租户管理等安全能力，为大数据平台提供安全防护和安全事件溯源能力。企业级大数据平台安全管理系统能力架构如图 4 所示。

（1）构建多租户权限管理体系。围绕以人为核心，建立租户、用户组、用户三大要素所组成的 3 层用户体系，对大数据平台进行立体式的用户管理，成功解决 Hadoop 平台原生安全认证能力过于单一，无法精细化、多样化地控制每一个用户权限的问题。3 层用户体系把组织、用户组、用户的概念融为一体，提供对平台资源统一分配、数据集中权限控制的能力，由上至下形成一条完整的管控链路，从全局实现平台资源和数据的统筹分配管理，从局部解决了租户内部资源管理与隔离。数据权限的管控与继承，既实现了租户与租户之间的完全隔离，也满足了租户内部对资源、数据灵活调配的定制化需求。现在多租户权限管理体系已经为全国 31 个省公司 167 个租户、1 343 个用户组的日常生产经营提供底层用户体系保障和安全管控服务。平台用户体系及资源管控如图 5 所示。

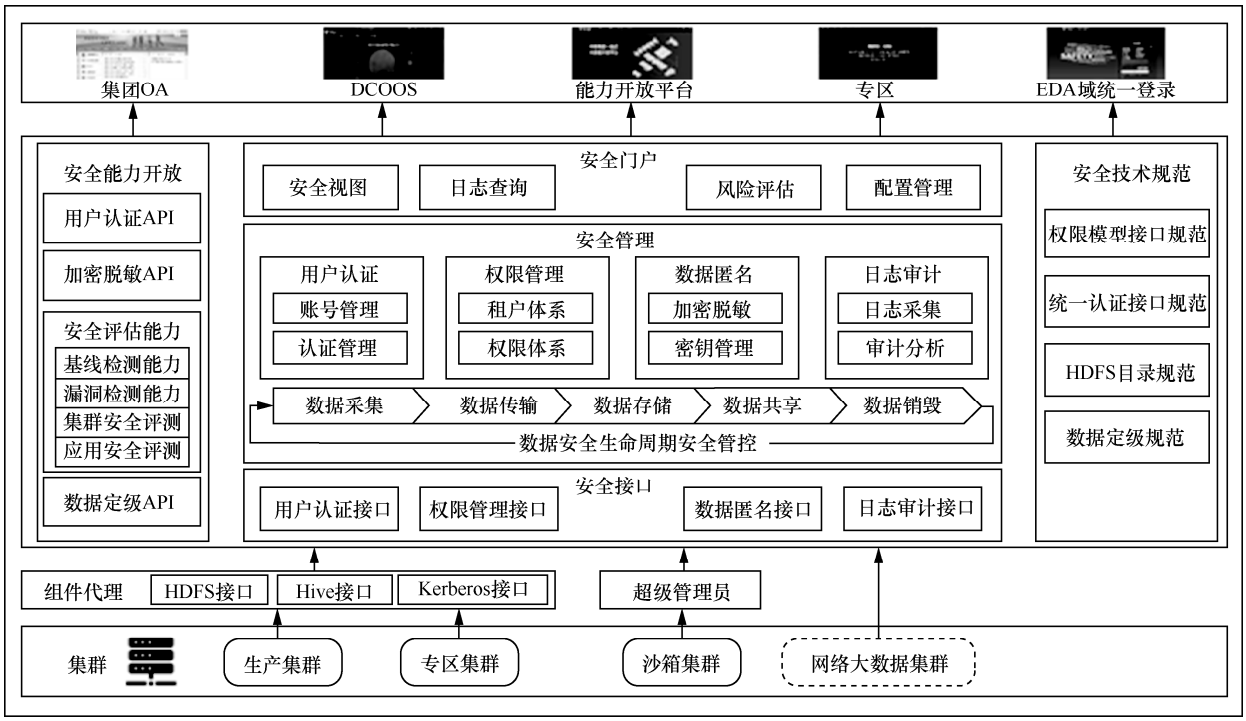

图 4　企业级大数据平台安全管理系统能力架构

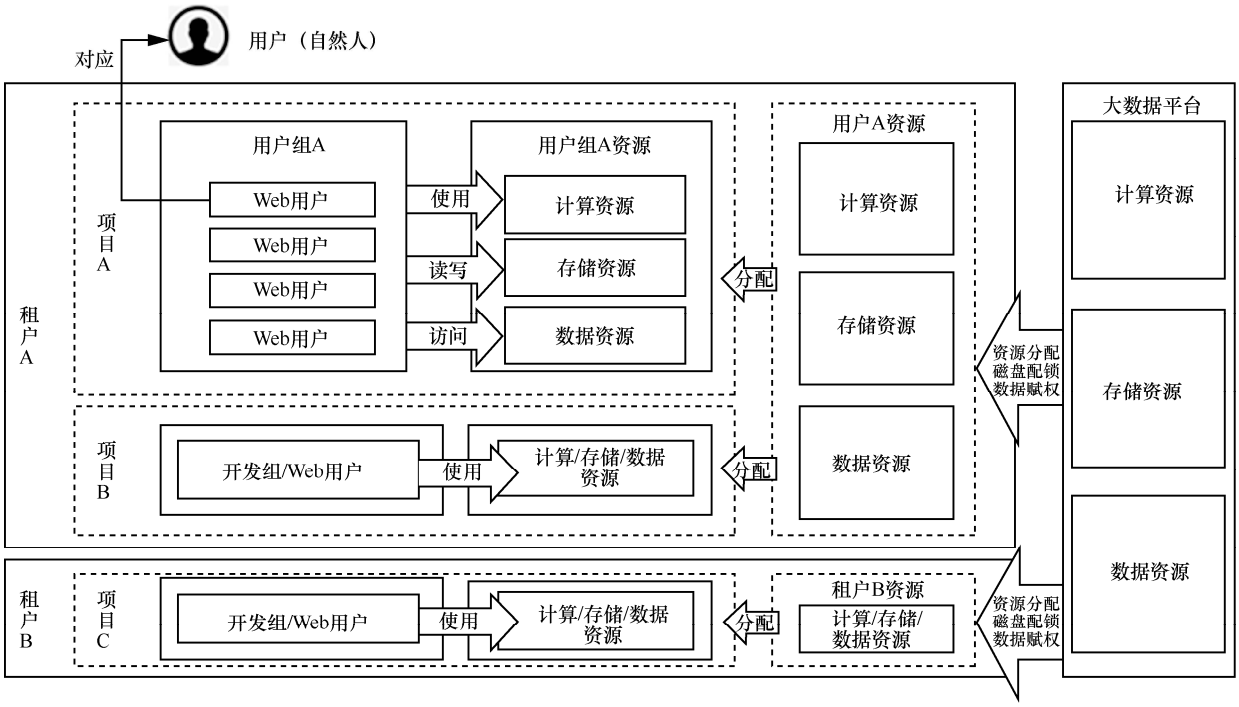

图 5　平台用户体系及资源管控

（2）统一身份认证管理，利用云认证平台提供大数据平台人脸、声纹、指纹、扫码等多因子认证服务，业务系统集中单点登录，实现对 14 个业务系统共计 25 000 个应用账号的统一管理，形成“一人一账号、一次登录通行访问”的用户便捷操作和安全保障能力。在大数据集群的身份认

证方面，Hadoop 主要支持简单机制和 Kerberos 机制两种身份认证机制[4]。简单机制根据用户的有效 UID 确认用户名，避免内部人员误操作。Kerberos 机制支持集群中服务器间的认证和客户端（client）到服务器的认证，严格控制数据输出，实现较强的安全性，同时保证较高的运行性能。技术上采用客户端/服务器结构与多层加密技术，密码和关键信息经过 3 层加密，先使用 base64 算法进行数据编码在经过 sha256 加密，其次再生成随机动态盐，密码和动态盐拼接在一块，经过 sha-224 类型的 SHA 算法加密生成最终的数据，用于防窃听、防 replay 攻击、保护数据完整性，使用对称密钥体制进行密钥存储，建立数据权限管理的基础安全环境。

（3）统一资产管理。对大数据平台内所有资产实施台账管理，与智能运维平台联动，建立“资产入网–资产变更–资产监视–资产退网”的流程，实现对主机、数据库、业务系统、网络拓扑图、业务系统互联关系等资产信息的全生命周期管控；在未知资产自动发现方面，通过端口扫描、协议探测等方式，可实现对网络中的未知资产对象的发现与基本信息侦测。验证试点全网数据资产测绘，通过集中式数据库 JDBC、CMDShell 等 API 连接方式实现定向采集，利用分布式终端 agent 进行本地脚本直采，实现 MySQL、Oracle、SQLServer 等主流关系型数据库以及 HBase、Hive、MongoDB、Redis 等主流大数据组件的资产数据采集，同时结合网络流量的采集监测进行 HTTP、FTP、SQL 等协议解析，可动态发现敏感数据的流动方向、使用热度等，结合平台资产信息可发现未登记、已退网等情况的异常资产，实现资产数据查漏补缺和动态更新；数据资产信息采集后通过周期性北向接口进行自动数据上报形成全网重要数据资产地图。

（4）统一日志审计管理。使用分布式数据抽取组件将数据进行加密传输，支持多种数据源类型可支持采集文件、网络数据、主机的审计和运行指标、堡垒机日志等，可自动化解析、规范转发以及数据库的日志。Lambda 架构如图 6 所示，使用经典的 Lambda 架构，数据传输到消息队列中，支持进行数据的无感分流；一方面使用分布式实时计算组件（Spark streaming）对接消息中间件进行实时数据指标的分析，形成用户行为轨迹、账号违规共享、执行高危指令、数据上传下载、异常时段登录、组件日志审计、Web 系统日志审计等能力;另一方面数据存储到 ES（elastic search）搜索引擎中，使用脚本结合 AI 挖掘建模技术，采用随机森林等算法对数据进行打标处理，根据多维评分模型，进行数据安全感知分析、威胁预判和预处理。

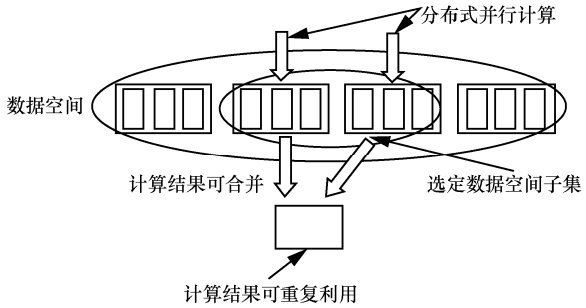

图 6　Lambda 架构

（5）提供数据匿名化解决方案。配套常用对称/非对称加解密算法 API，支持 aes/des/MD5/sm2/sm3/sm4/rc4 等多种加密能力，针对不同的业务场景可提供表级加密和字段级加密能力。大数据环境下的数据加密需要实现数据在静态存储及传输过程的加密保护，难点在于密钥管理。在 Hadoop2.6 的版本之后，HDFS 支持一种静态加密方式，应用层加密是一种基于加密区的透明加密方法，将需要加密的目录分解成若干个区，数据写入加密区和客户端读取数据时，数据被透明地加密和解密。对于动态的传输数据，对应 PRC、TCP/IP 和 HTTP，Hadoop 提供了不同的动态加密方法用以保证客户端和服务器传输的安全性。系统底层支持分布式的计算架构，利用分布式计算

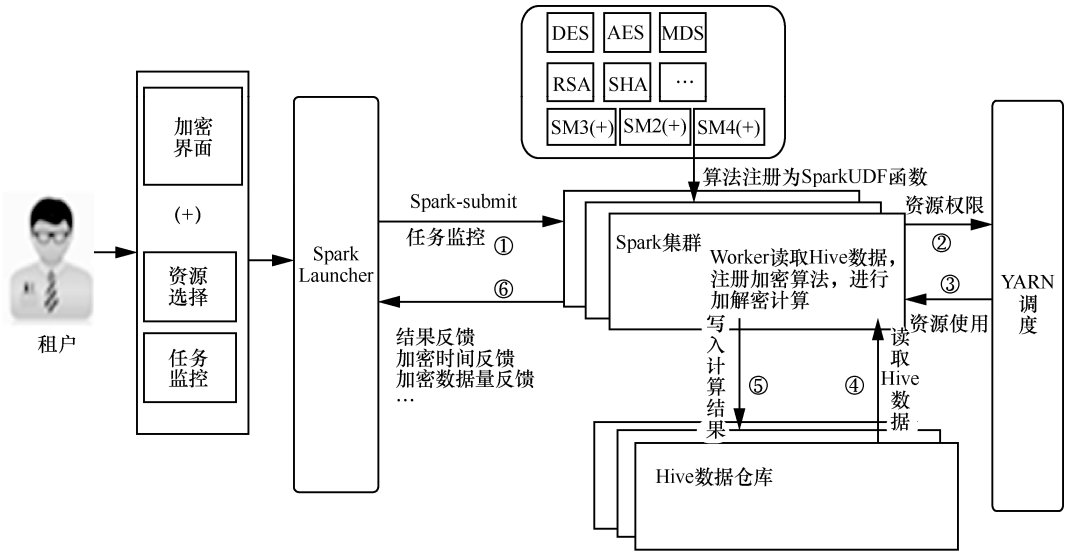

图 7　数据匿名架构

能够横向扩展的特性来提升数据加密性能。安全系统还对系统中所有的加/解密作业进行跟踪，记录每个作业的执行时间、运行状态、执行结果、相关数据等信息，以保证所有加/解密行为的有记可查。数据匿名架构如图 7 所示。

（6）构建统一的漏洞知识库。包括数据访问行为知识、用户访问组件行为知识、存储组件漏洞库等。从多个数据源获取攻击规则、软件漏洞样本、网络威胁情报、漏洞数据以及与计算机和网络安全相关的知识，对收集的知识进行统一化清洗处理，将分散的知识结构化为计算机可理解的知识库，通过五元组模型（包含概念、实例、关系、属性和规则），实现知识图谱化。通过将零散的安全阈值规则整合成体系化的安全漏洞知识库后，安全告警事件发现识别率提升 30%，预防潜在安全风险能力提升 20%。漏洞知识库构建架构如图 8 所示。

在解决数据汇聚和应用过程中大数据安全问题的同时，还有一些不足。一是重防范安全、轻共享安全，数据应用面临多种能力开放模式：如数据专区、挖掘建模、营销开发、服务封装，个人用户信息保护难度越来越大，传统的“一事一议”方式无法满足越来越多的数据开放需求，数据安全共享成为迫切需要解决的问题。二是安全风险监测智能化能力不足，依赖传统的基于规则过滤的黑名单制的日志审计，对疑似符合已知威胁模式/特征的行为产生告警，无法识别看似合法的风险隐患；检测水平取决于运营人员自身的经验和水平，缺少对 AI 新技术的有效使用。三是过于依赖网络和边界安全，缺乏数字化转型“企业边界正在瓦解，基于边界的安全防护体系正在失效”这一大背景下的应对措施。

4　大数据安全思考与展望

（1）引入联邦学习、区块链等技术在确保隐私安全前提下促进数据有序流通共享

隐私保护是建立在数据安全防护基础之上的保障用户个人信息的更深层次的安全要求。在数据共享方面，探索引入安全多方计算、联邦学习等隐私计算技术，在原始数据不出平台的情况下，与合作伙伴开展联合建模、联合营销、联合风控等场景的数据联合计算，实现“数据可用不可见”的安全体验；采用区块链技术进行数据服务调用的存证、授权、计费等，以确保数据计算和利用的合法合规，提供计算数据、过程的验证审计、数据监控等能力，保证计算过程真实可信、数据

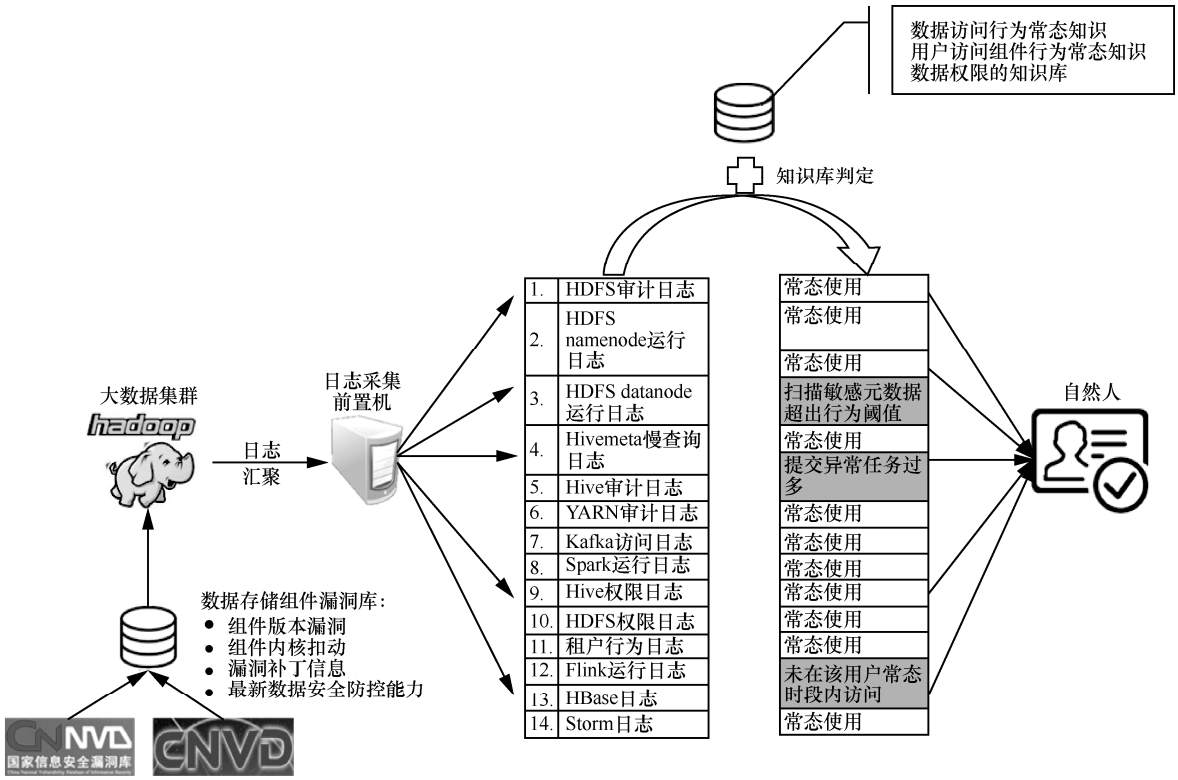

图 8　漏洞知识库构建架构

的真实性和数据质量；使用同态加密/部分同态加密技术，保护计算外包时的数据安全。在数据发布方面，利用数据匿名化算法（包括差分隐私、K 匿名、L 多样性、T 接近等）有条件地发布部分数据或数据的部分属性内容，达到隐私性和可用性的平衡。

（2）建立基于软件定义边界的零信任数据访问控制体系

基于 SDS（software defined security，软件定义安全）实现安全能力原子化、安全服务链编排，实现云网融合的安全产品与能力，提供多样化、可定制的云网安全服务。构建以身份为中心的信任体系和动态访问控制，建立全新的零信任微边界，引入角色挖掘、风险访问控制、半/非结构化数据的访问控制、针对隐私保护的访问控制、基于密码学的访问控制等新技术以实现对数据可信的访问控制，依据控制策略对资源进行不同的授权访问，从而保障数据资源在合法范围内得以有效使用和管理。持续开展信任评估，一旦环境发生变化就要去验证访问者是不是真实可信的，基于身份再次进行信任评估、基于环境的风险重新判定，基于行为的异常做出“检测+响应+阻止”，进而全面降低攻击者在网络中横向移动的风险。

（3）利用大数据和 AI 技术实现从被动防御到主动监测的转变

通过大数据分析、人工智能等技术，实现基于用户实体行为分析技术的审计监控，构建从数据采集、传输、使用、共享全链路的智能化风险检测能力[4]。在数据流转、接口监测方面，对 TCP/UDP 应用层服务及数据库协议进行解析和内容还原，基于文档指纹、图片特征、关键字匹配识别流量中的敏感数据，通过连续时间变量分析、概率分布对比（非参数检验/密度估计）和稀有度统计分析等离散变量、聚类 *K*-means/DBSCAN、离散森林（isolation forest）、LOF 等无监督学习算

法，构建和持续优化正常访问流量通道和行为模型，实现采集数据鉴别、传输接口、流动数据、共享接口、服务接口监测和风险预警能力。在数据使用和操作方面，通过机器学习算法和预定义规则对照行为基线判断用户行为是否异常，通过权限变化监控、用户安全风险综合评估，进行数据安全感知分析，对数据安全威胁预判、预处理，从源头上提升大数据安全防御水平，提升对未知威胁的防御能力和防御效率。

5　结束语

大数据时代，数据在流动和共享过程中不断创造新的价值。大数据不仅是数字化转型的重要驱动力，更是转型之后企业数字化发展的重要载体和工具。需要构建以数据为中心的、动态的数据安全防护体系，通过联邦学习、安全多方计算、人工智能和零信任的新技术研究应用，持续提升大数据安全效能，才能为企业数字化转型提供坚强保障与重要支撑。

参考文献：

[1] 全国信息安全标准化技术委员会.大数据安全标准化白皮书[R]. 2018.
National Technical Committee on Information Security of Standardization Administration. Big data security standardization white paper[R]. 2018.

[2] 刘志勇, 何忠江, 刘敬龙, 等. 统一数据湖建设研究和技术方案[J].电信科学, 2021, 37(1):121-128.
LIU Z Y, HE Z J, LIU J L, et al. Technology research and construction scheme of unified data lake[J]. Telecommunications Science, 2021, 37(1):121-128.

[3] 张锋军, 杨永刚, 李庆华, 等. 大数据安全研究综述[J]. 通信技术, 2020, 53(5): 1063-1076.
ZHANG F J, YANG Y G, LI Q H, et al. A survey of big data security[J]. Communications Technology, 2020, 53(5): 1063-1076.

[4] 中国信息通信研究院. 大数据安全白皮书[R].2018.
China Information and Communication Research Institute. Big data security white paper[R]. 2018.

[5] 中国国家标准化管理委员会. 大数据安全管理指南[R]. 2019.
Standardization Administration of China. Big data security management guide[R]. 2019.

[6] 中国国家标准化管理委员会. 大数据服务安全能力要求[R]. 2017.
Standardization Administration of China. Big data service security capability requirements[R]. 2017.

[作者简介]

刘志勇（1965− ），男，中国电信集团有限公司云网运营部、大数据和 AI 中心经理、教授级高级工程师，主要研究方向为云网融合、大数据和 AI 等。

何忠江（1980− ），男，现就职于中国电信集团有限公司云网运营部、大数据和 AI 中心，主要研究方向为大数据应用规划、建设和 AI 应用研发等。

阮宜龙（1977− ），男，现就职于中国电信集团有限公司云网运营部、大数据和 AI 中心，主要研究方向为大数据平台规划、建设、运营等。

单俊峰（1965− ），男，现就职于中国电信集团有限公司云网运营部、大数据和 AI 中心，主要研究方向为网络与信息安全、数据安全等。

张超（1980− ），男，现就职于中国电信集团有限公司云网运营部、大数据和 AI 中心，主要研究方向为大数据安全能力规划、建设与管理等。