Advances in Geosciences 地球科学前沿, 2026, 16(3), 321-329
Published Online March 2026 in Hans. https://www.hanspub.org/journal/ag
https://doi.org/10.12677/ag.2026.163030

Hans汉斯

海上油气勘探开发数据权限管控方案设计与实践

张金波*，封亚冬，田　婧，房甜甜，戴天琪，张翰羽

中海油研究总院有限责任公司，北京

收稿日期：2026年2月5日；录用日期：2026年3月4日；发布日期：2026年3月12日

摘　要

油气勘探开发过程中会产生大量敏感数据，大型数据管理平台的建设对做好敏感数据安全管控提出了更高要求，数据权限管理是其中最基础，同时也是最复杂的部分。针对该问题，通过分析油气勘探开发数据业务特点和数据权限管理需求，在经典的基于角色的访问控制(RBAC)和基于属性的访问控制(ABAC)权限管理模型基础上，提出了一种融合式数据权限管理方案。该方案在数据安全分类分级基础上，将用户和数据的多维属性进行提炼、对齐，并建立了同类属性信息匹配、校验机制，进而实现了从组织、角色、个人三个层次对不同安全级别的数据集、数据项、作用对象进行权限管控，且具备进一步灵活扩展能力。研究成果在中国海油勘探开发数据湖平台中落地实施，取得了良好应用效果，也可为其他同类大型数据管理平台数据权限管控问题提供借鉴。

关键词

海上油气，勘探开发，数据权限，RBAC，ABAC

Design and Practice of Data Permission Control Scheme for Offshore Oil and Gas Exploration and Development

Jinbo Zhang*, Yadong Feng, Jing Tian, Tiantian Fang, Tianqi Dai, Hanyu Zhang

CNOOC Research Institute Ltd., Beijing

Received: February 5, 2026; accepted: March 4, 2026; published: March 12, 2026

*第一作者。

文章引用: 张金波, 封亚冬, 田婧, 房甜甜, 戴天琪, 张翰羽. 海上油气勘探开发数据权限管控方案设计与实践[J]. 地球科学前沿, 2026, 16(3): 321-329. DOI: 10.12677/ag.2026.163030

Abstract

A large volume of sensitive data is generated during the process of oil and gas exploration and development, and the construction of large-scale data management platforms has raised higher requirements for the security control of such sensitive data. Data permission management is the most fundamental yet also the most complex component of this work. To address this issue, by analyzing the business characteristics of oil and gas exploration and development data and the requirements for data permission management, a hybrid data permission management scheme is proposed based on the classic Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models. On the basis of the classification and grading of data security, this scheme refines and aligns the multi-dimensional attributes of users and data, and establishes a matching and verification mechanism for homogeneous attribute information. Furthermore, it realizes permission control over data sets, data items and acting objects of different security levels from three dimensions: organization, role and individual, and features the capability for further flexible expansion. The research results have been implemented on the CNOOC Exploration and Development Data Lake Platform, achieving favorable application effects, and can also provide a reference for solving data permission control problems of other similar large-scale data management platforms.

Keywords

Offshore Oil and Gas, Exploration and Development, Data Permission, RBAC, ABAC

1. 引言

随着大数据、云计算、人工智能等新一代信息技术的迅猛发展，数据已被公认为第五生产要素[1]，成为推动现代社会快速变革、企业高速发展的核心战略资源。为更好激发数据要素价值，通过数智化转型实现高质量发展，国内外油气企业先后启动了大规模数据治理和大数据平台建设工作，并取得了显著成效[2]-[5]。

然而，数据的大规模集中也为油气企业带来了日益严峻的数据安全挑战。主要表现在以下几个方面：

(1) 油气行业数据安全工作起步较晚，国家层面目前还没有针对油气勘探开发领域数据安全分类分级出台权威性指导文件，各油气企业开展分类分级均基于自身业务现状和管理要求梳理，分类分级依靠人工经验，工作成果的科学性、完备性无法评判。

(2) 油气勘探开发业务链条长，跨专业、跨组织、跨层级数据交互、授权场景频繁。过去“系统烟囱”时代，每个系统独立管理其数据权限，技术难度相对简单，而到了大数据平台阶段，不同专业海量多源异构数据汇聚到一起之后，数据授权访问管理需求复杂度、技术难度大幅增加。

(3) 海上油气勘探开发相较于陆上情况更为复杂，多个方向地缘敏感度较高，相关数据的安全保密要求相比同类型陆上业务数据会更高，因此对数据权限管理要求不仅要“纵向”覆盖到敏感数据项，还要“横向”上进行行级别的区分，即权限管理的颗粒度要更细。

针对上述问题，本文在对海上油气勘探开发数据分类分级的基础上，综合运用基于角色的访问控制(RBAC)和基于属性的访问控制(ABAC)权限管理模型，设计搭建了一套适用于海上油气勘探开发大数据

平台数据权限管理要求的技术方案，并在中国海油勘探开发数据湖建设过程中进行了实际应用，取得了良好效果。

2. 数据分类分级与安全管控策略

2.1. 数据分类分级

分类分级是实现精细化数据安全管控的基石[6]。为解决当前缺乏权威指导性文件的问题，参照业内领先实践方法论[7] [8]，遵照国家法律[9] [10]及中国海油保密管理细则，对海上油气勘探开发数据进行了分类分级工作，确保划分依据可靠、划分结果科学。

按照业务大类进行划分，将海上油气勘探开发数据划分为勘探、开发、生产、工程建设、钻完井、储量、公共数据 7 大类。依据数据重要程度、敏感程度和遭到破坏(包括攻击、泄露、篡改、非法使用等)后对国家、社会、企业及个人造成的危害程度，将海上油气勘探开发数据划分为一般、重要、核心 3 个等级。具体如表 1、表 2 所示。

Table 1. Results of data classification for offshore oil and gas exploration and development
表 1. 海上油气勘探开发数据分类

分类	分类描述
勘探	油气发现阶段获取的地质与地球物理数据，包括地震采集与处理数据、野外地质调查记录、区域地质图、探井设计及录井、测井、测试原始数据等，用于识别潜在油气藏。
开发	油气藏开发方案研究与部署过程中产生的数据。涵盖油藏描述模型、数值模拟结果、开发井位部署方案、产能预测、经济评价参数等，用于优化开发策略和提高采收率。
生产	油气田日常生产活动中持续产生的运行与监测数据，包括生产报表类、生产实时类、作业调度类等，用于支撑油气田生产优化与智能运行。
工程建设	海上平台、海底管线、陆地终端等基础设施从设计、建造到安装全过程产生的工程数据，包括工程设计图纸、材料规格、施工日志、HSE(健康、安全与环境)记录、质量检验报告及竣工资料等。
钻完井	钻井与完井作业过程中产生的数据，包括设计数据、作业日报、井场实时数据、钻完井成果资料等，用于保障井筒完整性与后续生产。
储量	依据行业标准(如 PRMS 或 SPE-PRMS)评估和上报的油气资源与储量数据。包括原始地质储量(OGIP)、可采储量、储量分类(探明、概算、可能)、动态储量更新记录及评审备案文件等，是企业资产估值与国家资源监管的关键依据。
公共数据	主数据、参考数据等。

Table 2. Basis for data classification and grading in offshore oil and gas exploration and development
表 2. 海上油气勘探开发数据分级

分级	分级描述
一般数据	数据失泄密、篡改或丢失时，可能对勘探开发业务运行造成一般性影响。
重要数据	数据失泄密、篡改或丢失时，可能对集团公司造成一定负面影响或经济损失；对勘探开发核心业务运行造成重大影响，如：多个系统内特定业务流程或数据服务故障。
核心数据	数据失泄密、篡改或丢失时，可能对集团公司或行业造成极大负面影响或巨大经济损失；对勘探开发数据湖核心业务运行造成极大影响。

2.2. 数据安全管控策略

遵照国家法律[9] [10]、上级监管部门数据安全规范[11] [12]以及中国海油集团公司数据安全管理要求，制定海上油气勘探开发数据安全管控策略，具体如表 3 所示。

Table 3. Data security control strategies for offshore oil and gas exploration and development
表 3. 海上油气勘探开发数据安全管控策略

数据安全定级	管控目标	用户访问权限要求
核心	具体包含核心数据列、核心数据行两个方面，默认只对单个用户共享。无权限用户访问核心数据列时脱敏处理。	三级
重要	默认在所属二级单位范围内共享，按照用户所在角色组进行控制，无权限用户访问重要数据时进行脱敏处理。	三级、二级
一般	默认在中国海洋石油有限公司范围内无条件共享。	三级、二级、一级

注：同类型但属于敏感区域的数据须提级管理。

3. 数据权限管控方案总体设计

3.1. 数据权限管理模型选择

在数据安全行业，基于角色的访问控制模型(Role-Based Access Control, RBAC)和基于属性的访问控制模型(Attribute-Based Access Control, ABAC)是两种广泛应用的数据访问控制模型，两者在概念、实现方式上有所不同[13]。

RBAC 是通过将用户与角色关联，并将角色与权限绑定，来实现对用户访问资源的控制[14]-[20]。其优点是更加直观与简单，简化了权限管理的复杂性，降低了管理成本，易于理解和实施。缺点是无法满足某些需要对数据权限精细化控制的场景，且当角色或资源的权限发生变化时，需要手动调整用户的角色以及对应角色的数据权限，长期积累后角色管理复杂度会不断上升，进而导致管理失效。

ABAC 是通过动态评估用户、环境、操作和对象等属性是否满足特定策略来决定是否授权访问[21]-[25]。其优点是允许根据更加详细的属性和条件来制定授权策略，从而实现对数据访问控制的精确控制，且当用户的属性发生变化时，模型能够自动调整权限设置，无需手动干预。缺点是技术实现相对复杂，访问安全策略配置及权限校验引擎的稳定性、可扩展性对技术要求较高。

为满足海上油气勘探开发场景下对数据安全管控的严格要求，在兼顾细粒度、灵活性的访问控制能力与系统运维管理复杂度之间取得平衡，本文提出融合 ABAC 与 RBAC 的混合授权模型。该模型充分发挥 ABAC 在细粒度策略表达和动态属性匹配方面的优势，同时保留 RBAC 在权限组织与管理效率上的适用性。通过自动识别并验证用户属性与数据资源属性之间的匹配关系，系统能够在保障高安全性的同时，实现高效、便捷的数据访问控制，从而达成安全性与可用性的协同优化。

3.2. 数据权限管理前置工作梳理

3.2.1. 用户属性梳理

根据数据权限管理目标，将用户属性分为所属组织、所属角色、所属等级、操作权限 4 大类，如表 4 所示。其中，所属组织记录用户所在的组织机构层级，如：总部/勘探开发部、总院/数据资源中心等。所属角色记录用户岗位信息，如：管理、技术/勘探、技术/开发等。所属等级记录用户当前所拥有的权限等级，如：一级、二级、三级。操作权限记录用户对所访问数据的增删改查权限类型，如：R、C/R、C/R/U/D 等。

Table 4. Schematic diagram of user attribute matrix
表 4. 用户属性矩阵

用户	组织	角色	权限等级(0, I, II, III)	操作权限(CRUD)
user1	总部\勘探开发部	管理	III级	R
user2	总部\科信部	管理	II级	R
user3	总院\勘探开发院	技术\勘探	II级	C/R
user4	总院\勘探开发院	技术\勘探	I级	C/R
user5	总院\数据中心	数据治理	I级	U/D
user6	总院\数据中心	系统开发	I级	R
user7	天津	管理	III级	R
user8	天津	管理	II级	R
user9	天津	管理	I级	R
user10	上海	技术\勘探	III级	C/R
user11	上海	技术开发	II级	C/R
user12	深圳	技术\生产	I级	C/R
user13	湛江	技术\钻完井	0 级	C/R
user14	湛江	数据治理	0 级	U/D
user15	海南	系统开发	0 级	R

3.2.2. 数据属性梳理

根据数据分类结果，并结合海上油气勘探开发业务特点，将数据属性分为所属组织、所属专业、所属安全分级、是否敏感区 4 类，如表 5 所示。其中，所属组织记录数据在勘探开发业务流程中的归属和管理责任，如所属分公司、作业区、项目等，组织属性可以用于确定数据所有权、访问权限等，是数据权限设定和管理的关键因素。所属专业描述了数据所属数据分类信息，如：勘探、开发、生产、钻完井等。所属安全级别记录了数据的安全定级结果。是否敏感区根据该数据关联主数据是否为敏感数据进行判断，如判断为是将在现有安全定级基础上提级管理。

Table 5. Schematic diagram of data attribute matrix
表 5. 数据属性矩阵示意

数据	所属组织	所属专业	行级主数据敏感特征	列级(一般、重要、核心)
数据 1	深圳分公司	勘探	敏感	核心
数据 2	海南分公司	勘探	敏感	重要
数据 3	湛江分公司	开发	敏感	一般
数据 4	湛江分公司	生产	非敏感	核心
数据 5	天津分公司	储量	非敏感	重要
数据 6	上海分公司	工程建设	非敏感	一般

3.2.3. 数据权限校验逻辑梳理

根据用户属性和数据属性梳理情况，进一步梳理权限校验逻辑。当用户通过大数据平台数据查询工具对企业数据进行访问时，数据权限校验引擎将根据用户所在角色组自动提取用户属性信息，并与目标数据属性信息进行比对。当比对结果判定为符合访问要求时返回正确结果；当比对结果判定为不符合访问要求时，调用动态脱敏工具，对不符合要求的数据进行脱敏后返回给用户。属性校验工具引擎工作过程如图 1 所示，校验逻辑如表 6 所示。

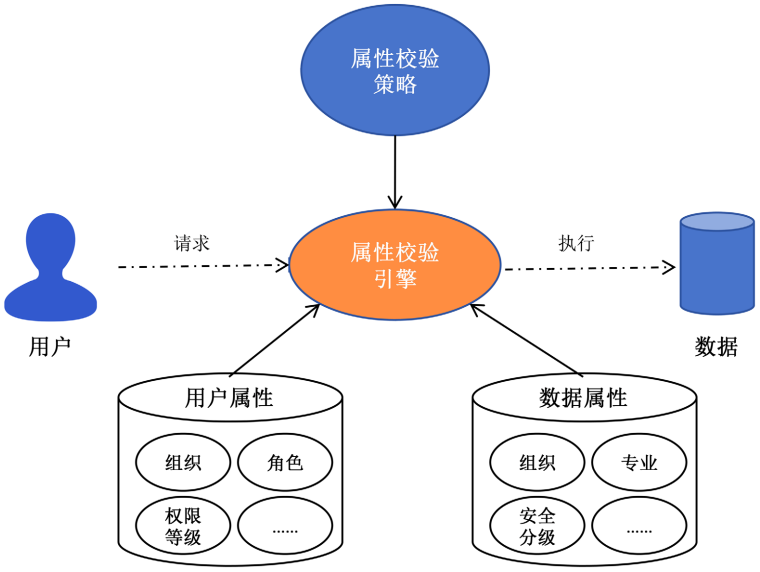

Figure 1. Schematic diagram of the working process of data permission verification engine
图 1. 数据权限校验引擎工作过程示意图

Table 6. Diagram of attribute verification
表 6. 属性校验逻辑

用户属性	数据属性	匹配	不匹配	策略规则描述
组织	组织	≥	<	1) 总部、总院可查看所有组织数据； 2) 分公司只可查看各自分公司数据。
角色	专业	≥		1) 管理、技术、数据治理、系统开发可查看所有专业数据； 2) 技术专业只可查看所属专业数据。
权限等级	敏感特征安全分级	≥		0 级：可查看非敏感主数据，一般数据集； I级：可查看非敏感主数据，重要数据集； II级：可查看非敏感主数据，核心数据集； III级：可查看敏感主数据，核心数据集。

3.3. 技术实现与性能测试

根据上述安全管控策略和全校校验逻辑梳理情况，以用户登录数据平台使用综合查询功能为目标场景，制定动态脱敏详细技术方案(图 2)，并据此完成功能开发。具体实现逻辑分为以下 7 个步骤：

1) 用户登录数据平台，点击综合查询工具，进入页面输入查询条件。

2) 数据平台综合查询工具根据用户输入的查询条件，调用相关数据查询服务，并自动生成执行 sql

语句与大数据平台存储软件(如中国电子云信创数据产品 CeaSQL、CeaSQL-DW、CeaInsight 等，也可与开源大数据产品如 Hadoop 系列、Flink 系列等)进行交互。

3) 查询 sql 执行完毕，获取数据反馈大数据平台获取到数据返回结果。

4) 属性校验引擎对返回的数据属性信息进行拆解分析，并查询返回数据对应的数据安全策略，如字符型数据项部分遮蔽、数字型数据项遮蔽/数值转换等。

5) 数据平台安全模块将实现配置好的安全策略以及查询结果数据的分类分级信息返回给属性校验引擎。

6) 属性校验引擎对用户属性和数据属性，按表 6 所示校验逻辑规则进行比对。对于符合权限管控条件的数据直接返回查询模块；对于不符合权限管控条件的数据，动态调用脱敏组件，按照既定脱敏策略对敏感数据进行脱敏后返回查询模块。

7) 查询模块完成数据接收之后，按照实际情况将用户有权访问的数据展示到查询界面中。

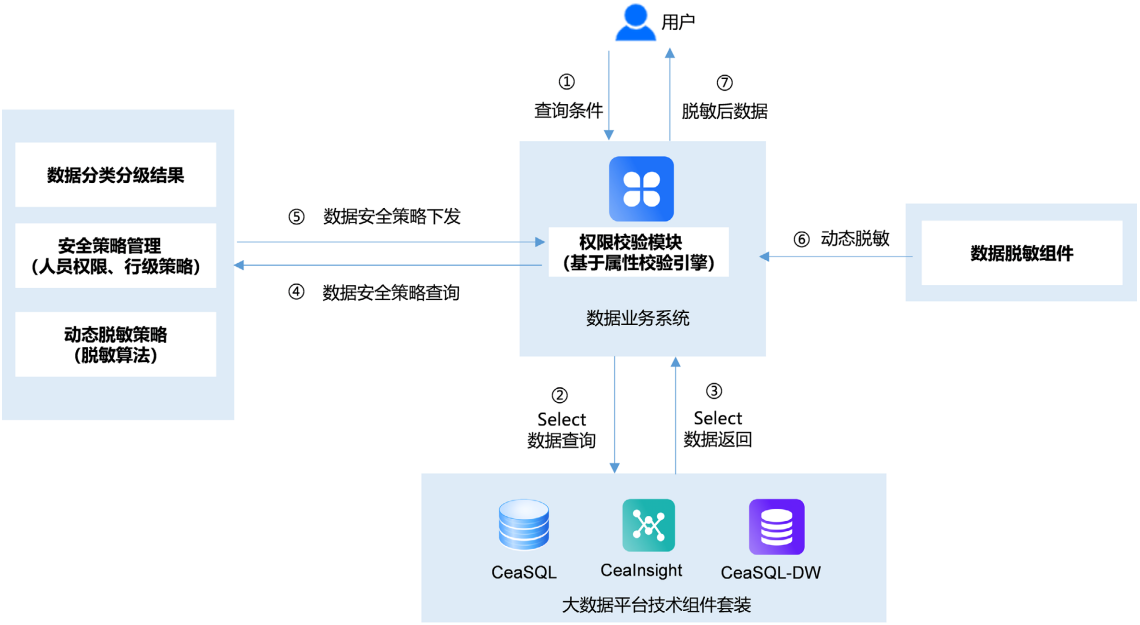

Figure 2. Process of permission verification and dynamic data masking for users utilizing the integrated query function
图 2. 用户使用综合查询功能权限校验及动态脱敏流程

为评估上述所提权限校验机制的运行开销，功能开发完成后在内网大数据平台测试环境进行了部署验证。验证结果表明，在典型业务查询负载下，启用权限校验引擎后单次查询延迟增加 3%，主要消耗在执行 sql 转化和调用脱敏插件过程中，吞吐量保持不变。这证明该方案在保障数据安全的同时，对系统性能影响可控，具备工程落地可行性。

4. 海上油气勘探开发数据权限管控实践

基于上述数据权限管控设计方案，中国海油在勘探开发数据湖建设过程中研发并部署了数据权限校验与管理工具，并成功实现了该工具与综合查询、自助分析及动态脱敏等核心数据服务模块的深度集成与联动，并首次在国内油气勘探开发领域实现了面向行级数据的细粒度动态访问控制(图 3)，有效支撑了敏感数据在复杂业务场景下的按需、按权、按上下文安全访问，显著提升了数据安全治理能力与业务使用效率的协同水平。

序号	井	设计井口横坐标(m)	设计井口纵坐标(m)	设计井口经度(°)	设计井口纬度(°)	设计完钻井深(m)
1	W[redacted]H	[redacted]	[redacted]	[redacted]	[redacted]	5600.00
2	W[redacted]H	-88888	-88888	-88888	-88888	5655.00
3	W[redacted]	-88888	-88888	-88888	-88888	3860.00
4	W[redacted]H	[redacted]	[redacted]	[redacted]	[redacted]	4525.00

Figure 3. Effect diagram of dynamic desensitization access control for row-level data in offshore oil and gas exploration and development
图 3. 海上油气勘探开发行级数据动态脱敏访问控制效果图

在实际运行过程中，本文所述解决方案可满足用户跨组织授权、临时授权、按对象授权、权限委托等多维度复杂场景，相较于单纯运用 RBAC 管理模式有较大提升，具体如表 7 所示。

Table 7. Support for complex scenarios in the access control module of CNOOC exploration and development data lake
表 7. 中国海油勘探开发数据湖权限管控模块复杂场景支撑情况表

场景名称	场景举例	面临挑战	传统 RBAC 解决方案	本解决方案
跨组织授权	员工临时借调用数需求	实时更新困难	频繁新建角色	无需专门配置，权限随属性变化同步更新
临时授权	员工参与项目用数需求	过期自动回收困难	频繁改动角色有效期，无法精确到人	可单独设置某时段安全等级，到期自动作废收回
按对象授权	相邻跨组织区块用数需求	细颗粒度管控困难	频繁新建角色组，维护困难	独立设置不同区块、不同井安全等级，稳定不变
权限委托	各二级单位自主授权	逐级授权困难	不支持	支持基于用户属性的分级授权

数据权限校验与管理工具自 2024 年 Q1 在勘探开发数据湖平台上线以来，已累计触发高风险越权访问数据脱敏 8237 次，覆盖井位实测坐标、潜力区块储量信息等敏感数据。用户可在自己所属职责属性范围内最大程度获取数据资源，避免了大量因授权不合理而导致的权限申请工作量，提升了用户体验。同时，数据授权流程实现 100%线上化，数据权限审批周期从平均 6.2 天压缩至 0.8 天，显著提升数据服务效率与合规水平。

5. 总结

数据安全是实现数据高效共享流通与价值释放的前提与基石。本文所提出的 ABAC 与 RBAC 混合授权模型解决方案，不仅显著简化了大数据平台数据权限管理架构，还通过属性驱动的动态访问控制机制，有效降低了策略维护成本，提升了管理效率。运维人员与管理员仅需在权限策略工具中基于用户属性与资源属性定义访问规则，即可实现对数据访问行为的灵活、精准控制。实际应用表明，该方法可在大数据平台数据权限管控中取得良好效果，为油气能源领域构建可信、智能、高效的数据安全运营环境提供有力支撑。

基金项目

中国海洋石油集团有限公司“十四五”重大科技项目“智能油田关键技术(编号：KJGG-2024-15)”；中国海洋石油有限公司信息化项目“勘探开发数据湖平台智能分析工具建设”(中海油科数[2025] 284 号)

部分研究成果。

参考文献

[1] 黄阳华, 张津硕, 张钟文. 基于数据要素的数字经济增长与核算理论[J]. 中国人民大学学报, 2026(1): 37-47.

[2] 律红洲, 黄希彧. bp 公司数字化转型经验与启示[J]. 世界石油工业, 2022, 29(6): 35-39.

[3] 曾涛, 刘晗光, 高坚. 斯伦贝谢公司数字化转型的经验与启示[J]. 国际石油经济, 2021, 29(1): 94-99.

[4] 夏聪, 刘凡, 梁远明. 石油行业信息化建设与需求的策略探讨[J]. 化工管理, 2023(17): 84-87.

[5] 蒋楠. 石化企业数据治理方法及应用[J]. 炼油技术与工程, 2024, 54(8): 46-50.

[6] 帅训波, 陈东, 董之光, 贾文清, 叶铭, 李青. 石油石化行业信息系统安全技术标准体系建设[J]. 石油与天然气化工, 2026, 55(1): 105-112.

[7] 袁康, 鄢浩宇. 数据分类分级保护的逻辑厘定与制度构建——以重要数据识别和管控为中心[J]. 中国科技论坛, 2022(7): 167-177.

[8] 商希雪, 韩海庭. 数据分类分级治理规范的体系化建构[J]. 电子政务, 2022(10): 75-87.

[9] 中华人民共和国主席令第 84 号. 中华人民共和国数据安全法[EB/OL]. http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html, 2021-06-10.

[10] 中华人民共和国主席令第 53 号. 中华人民共和国网络安全法[EB/OL]. https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm, 2016-11-07.

[11] 全国信息安全标准化技术委员会. 网络安全标准实践指南——网络数据分类分级指引[EB/OL]. https://www.tc260.org.cn/portal/article/303/7f3487831107464c99aa9d094eeeb995, 2021-12-01.

[12] 国家市场监督管理总局, 国家标准化管理委员会. GB/T22240-2020 信息安全技术网络安全等级保护定级指南[S]. 北京: 中国标准出版社, 2020-04-28.

[13] 李凤华, 苏铓, 史国振, 马建峰. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805-813.

[14] 徐晨, 朱润酥, 吴振洲, 纪添, 李晨希. 访问控制安全模型研究[J]. 网络空间安全, 2024, 15(1): 97-102.

[15] Liu, Y.A. and Stoller, S.D. (2005) Role-Based Access Control: A Simplified Specification. Technical Report DAR 05-24, Computer Science Department, SUNY Stony Brook.

[16] Jha, S., Li, N., Tripunitara, M., *et al*. (2008) Towards Formal Verification of Role-Based Access Control Policies. *IEEE Transactions on Dependable and Secure Computing*, **5**, 242-255. https://doi.org/10.1109/tdsc.2007.70225

[17] 李梁磊, 邵立嵩, 王传勇, 刘勇, 王坤. 面向泛在网络的 CA-RBAC 访问控制[J]. 网络空间安全, 2017, 8(Z2): 48-54.

[18] Rajpoot, Q.M., Jensen, C.D. and Krishnan, R. (2015) Integrating Attributes into Role-Based Access Control. In: *Lecture Notes in Computer Science*, Springer, 242-249. https://doi.org/10.1007/978-3-319-20810-7_17

[19] Fries, S., Falk, R. and Bisale, C. (2017) Role-Based Access Control in the Digital Grid—A Review of Requirements and Discussion of Solution Approaches. *International Journal on Advances in Security*, **10**, 223-232.

[20] 丁睿, 陈浩, 马杰. 一种基于零信任的威胁感知访问控制方法[J]. 网络空间安全, 2021, 12(Z6): 43-48.

[21] 夏桐, 袁凌云, 谢天玉. 融合聚类和结构优化的属性访问控制策略评估[J]. 计算机工程与科学, 2025, 47(12): 2169-2180.

[22] Riad, K. and Cheng, J. (2021) Adaptive XACML Access Policies for Heterogeneous Distributed IoT Environments. *Information Sciences*, **548**, 135-152. https://doi.org/10.1016/j.ins.2020.09.051

[23] Deng, F., Yu, Z., Liu, W., Luo, X., Fu, Y., Qiang, B., *et al*. (2021) An Efficient Policy Evaluation Engine for XACML Policy Management. *Information Sciences*, **547**, 1105-1121. https://doi.org/10.1016/j.ins.2020.08.044

[24] 张焕, 侯明星, 刘光娜, 史颖. 基于动态数据敏感等级的大数据细粒度访问控制模型[J]. 计算机科学, 2026, 53(2): 187-195.

[25] 王小铁, 练斌. 一种基于属性的动态访问控制技术分析[J]. 集成电路应用, 2025, 42(3): 110-111.