

大模型与区块链双引擎驱动的数据字段级全生命周期安全治理技术研究

——中国电信“先审后用”实践验证

文◆中国电信股份有限公司

中国电信股份有限公司江苏分公司

中国电信股份有限公司

张侃

魏渊

武姗姗 渠凯

引言

数据要素市场化进程加速，企业取数用数呈现高频化、场景多元化的特征。在此背景下，中国电信创新性提出“先审后用”数据安全管控理念，构建融合大语言模型（LLM）与区块链技术的全生命周期安全治理体系。该体系通过垂直混合专家模型（MoE）构建智能研判引擎（AIAgent），实现审核与策略的动态优化，并依托区块链智能合约实现操作存证与权责追溯，形成“智能研判—可信执行—安全流通”三级协同机制，最终实现字段级细粒度数据管控目标。实践表明，该系统显著提升了数据安全治理效率与合规水平，具备行业应用与推广价值。

1 “先审后用”理念与核心问题解析

1.1 “先审后用”定义

“先审后用”是中国电信在数据安全领域首创的核心管控理念，核心是构建“事前智能预审、事中精准校验、事后动态追溯”的取数用数全生命周期闭环管控体系^[1]。其聚焦“审”与“用”关键节点，通过“管理+技术”协同驱动，确保数据从申请、审批、流转至销毁的全流程合规，形成企业级数据安全专业化治理范式。

1.2 企业取数用数的核心问题

数据要素市场化背景下，企业取数用数面临四大痛点。

（1）审核效率低。依赖人工校验高频跨场景取数请求，平均审核响应时间超4h，效率低且易出错。

（2）策略刚性。传统系统管控粗放，缺乏数据字段级细粒度管控，且规则策略僵化，难以满足动态业务需求。

（3）流程断裂。数据出口分散、流程割裂，导致跨部门数据共享处理时间长，制约数据价值释放。

（4）责任溯源问题。操作日志分散、系统信息隔离，数据泄露后异常追溯超过3天，权责难落实到人。

2 研究目标与创新价值

2.1 研究目标

针对数据取用环节中业务多元、主体复杂与流动高频的特点，本研究以电信现有体系为基础，构建“双引擎三层次”协同架构，支撑“先审后用”全生命周期管理，推动数据治理由被动防御转向主动防控，夯实数据要素市场化安全基础^[2]。

2.1.1 双引擎

一是大模型引擎，基于混合专家模型的智能研判引擎，实现需求语义拆解、敏感数据识别、字段级合规决策以及审计策略动态优化。二是区块链引擎，其依托智能合约实现业务规则固化、操作存证与权责追溯。

2.1.2 三层次

智能研判层实现审核要素全

【作者简介】张侃（1970—），男，江苏苏州人，博士研究生，教授级高级工程师，研究方向：信息通信、网信安全。

流程穿透，驱动需求申请到合规判定的自动化决策；可信执行层依托区块链智能合约固化业务逻辑，结合非对称加密与共识机制保障操作可信存证；安全流通层通过动态加密删除原文、仅流转受控副本，依托三权分立与实时鉴权机制，在双引擎协同下确保数据明文不落地，文件使用全生命周期可知、可管、可控。

2.2 核心创新点

（1）架构创新。构建“双引擎三层次”架构，融合大模型智能合规研判与区块链可信存证，突破传统粗粒度管理，实现字段级全生命周期细粒度管控。

（2）机制创新。建立“以链治数”（规则固化与可信追溯）与“以智促治”（动态研判与策略优化）协同机制，破解“技术可信”与“管理可控”融合难题。

（3）范式创新。实现企业级数据字段级管控与全生命周期安全治理，推动数据安全从“被动防御”向“主动防控”转型。

3 研究方法与技术架构

3.1 总体技术架构

以大模型与区块链为双引擎，构建“智能审核层—可信执行层—安全流通层”三层次架构，各层通过接口动态协同，形成“研判—执行—流通”闭环（见图1）。

3.2 核心模块设计

3.2.1 智能研判引擎：需求语义拆解—合规动态研判—策略自适应生成

基于 MoE 构建专用智能研判引擎，以解决人工审核低效与动态合规问题。该引擎实现审核要素全流程智能贯穿，通过 LLM 的语义理解能力驱动非结构化需求的智能语义拆解，自动完成需求合规研判与智能决策。融合

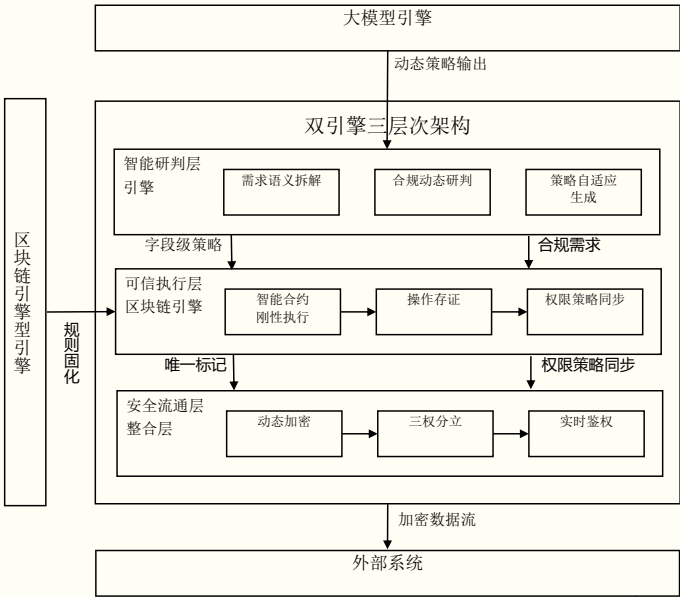


图1“双引擎三层次”技术架构

RLAIF 框架，以“合规匹配度与风险权重动态平衡”为核心设计奖励函数（如融合规则匹配度与敏感字段泄漏风险量化值），驱动审计与稽核策略的动态生成及自适应优化，破解合规性动态适配难题。引擎采用 HIL 架构，通过静态 / 动态断点控制高风险操作，保障数据安全。在技术实现上，AIAgent 采用多智能体架构，支持模块化设计，可独立处理合规规则解析、风险评估、策略生成等子任务，有效提升系统灵活性。

（1）LLM 模型选择。采用经过大量电信领域典型样例以及数据安全法规专项训练的自研模型，能够准确理解数据安全合规要求。模型基于 Transformer 架构，具备强大的自然语言处理能力，可解析复杂的合规规则与条款。

（2）RLAIF 训练机制。奖励函数定义为“ $R = \alpha \cdot C_{\text{合规}} + \beta \cdot (1 - R_{\text{风险}}) + \gamma \cdot R_{\text{需求}} + \delta \cdot S$ ”范围，其中 $\alpha, \beta, \gamma, \delta$ 为权重系数（ $\alpha + \beta + \gamma + \delta = 1$ ，且 $\alpha, \beta, \gamma, \delta \in [0, 1]$ ）。各参数含义如下。

C 合规表示与数据安全法规及业务规则的匹配度（取值范围 [0,1]，值越高匹配度越好）； R 风险表示敏感字段泄漏风险量化值（取值范围 [0,1]，值越高风险越高，通过 $1 - R$ 风险转换为正向奖励）； $R_{\text{需求}}$ 表示数据使用需求的合理性（取值范围 [0,1]，值越高表明需求与业务场景的契合度越高）； S 范围表示数据获取范围的最小化程度（取值范围 [0,1]，值越高表明越符合“最小必要”原则）。

训练数据采用多源融合策略，以近一周全量历史审批工单以及分层采样罕见场景，融合典型样例，形成覆盖取数用数全生命周期的训练样本集。基于上述数据，通过 RLAIF 框架持续优化策略生成算法，实现合规判定精度、风险防控能力、需求匹配度与范围最小化水平的动态平衡。

（3）策略建模机制。采用基于规则的策略建模机制，将合规规则转化为可执行的策略模型。包含数据分类分级规则、访问控制规则、审计策略生成规则等，可根据数据敏感性和业务需求动态调整。

（4）审核要素台账协同治理机制。通过审核要素台账（含内外部人员系统权限台账、用数合规台账等关键审核要素）贯通业务逻辑与数据

操作,结合区块链技术实现跨主体权责协同,破解“前后端割裂”痛点,打破信息孤岛。

3.2.2 可信执行与追溯引擎:规则固化与全链路可信存证

依托区块链智能合约技术载体(“合约即制度”)固化业务逻辑,依托密码学哈希、共识机制、非对称加密确保日志不可篡,通过“链式结构+时间戳”实现操作全链路责任可追溯,解决责任溯源与操作可信问题。

(1) 规则固化。将“先审后用”业务逻辑写入智能合约,确保审批规则刚性执行,避免人为干预。

(2) 全链路存证。将需求申请、审批结果、取数操作等关键节点日志上链,结合时间戳与哈希加密,实现操作“不可篡改、全程可溯”,异常行为定位时间缩短至12min以内。

(3) 权限同步。实时同步跨系统权限信息(如合作方账号权限变更),确保“取数人权限与审批结果一致”。

3.2.3 安全流通机制:数据明文不落地与使用全周期可控

该机制通过计算数据摘要生成唯一数据指纹并与区块链日志绑定,在保障数据明文不落地的前提下,实现全生命周期确权分权与权属可验证。在数据文件流转环节,执行导出加密并自动删除原文,仅流转加密受控副本;结合实时鉴权体系实施细粒度访问控制,实现流过程的精细化管控与明文不落地,最终达成数据全生命周期可知、可管、可控。

(1) 动态加密。采用国密SM4对称加密与SM2非对称加密结合方案,数据导出时自动生成加密副本并删除明文,确保“明文不落地”。

(2) 三权分立。明确数据所有权、管理权、使用权,形成层级授权链路,实现权限分离与可控分配,避免权限滥用。

(3) 实时鉴权。根据用户角色、操作环境等动态匹配权限,仅允许访问审批范围内的字段级数据。

3.3 核心流程说明

字段级数据全生命周期管控核心流程按“申请—研判—执行—流通—销毁”全链路闭环设计,关键操作环节如下。

(1) 需求申请。用户提交数据使用请求,系统自动触发治理流程。

(2) 智能拆解。大模型引擎对非结构化需求进行语义解析,识别敏感字段与合规要素。

(3) 合规研判。基于混合专家模型与实时策略库,生成字段级合规判定结果。

(4) 策略优化。通过RLAIF奖励函数($R = \alpha \cdot C_{\text{合规}} + \beta \cdot (1 - R_{\text{风险}}) + \gamma \cdot R_{\text{需求}} + \delta \cdot S_{\text{范围}}$)实现策略动态调优。

(5) 动态加密与流通。采用SM4/SM2混合加密机制,生成加密副本并删除明文,确保数据“明文不落地”,并通过实时鉴权实现细粒度访问控制。

4 案例验证与结果分析

4.1 验证场景与指标设计

选取江苏电信、贵州电信以及天翼物联网公司作为试点,涵盖内部取数合规审核、合作方用数权限管控与物联网跨省数据流通审计三类场

景,并从效率、安全与可控性3个维度设定了包括审核响应时间、合规准确率以及追溯成功率等量化指标。

4.2 实践验证与结果分析

本体系在三类典型业务场景中取得显著成效。

(1) 江苏电信(内部取数场景)。审核响应时间由4h缩短至90min,效率提升60%;字段级管控覆盖率达到100%;依托区块链全链路存证,实现异常操作100%溯源定责。

(2) 天翼物联网公司(跨省数据流通场景)。支持日均百万级请求处理,无延迟响应;明文泄漏率为零,杜绝“搭车出数”风险;跨省操作追溯成功率达100%。

(3) 贵州电信(合作方用数场景)。大模型预审风险识别率提升40%,合作方违规操作率下降72%,实现全流程穿透式管理,权限与合同、人员信息完全对齐。

结语

本研究通过大模型与区块链协同,实现了数据字段级全生命周期治理,有效解决企业数据使用中的合规、效率与溯源问题。未来将重点优化模型安全与跨行业适配性,推动“先审后用”成为行业标准。

引用

- [1] 吴沈括.2022年度国内数据安全的现状与发展:挑战与对策[J].信息安全研究,2023,9(6):512-528.
- [2] He T,Zhang Z,Sun J,et al. Qwen2.5:Advancing Large Language Models with Efficient Training[J].IEEE Transactions on Knowledge and Data Engineering,2024,36(5):2100-2115.