网安卫谷
WEIGUTECH

让安全随手可得

卫谷智+大模型应用产品

技术白皮书

V1.2

2026 年 05 月 22 日

浙江网安卫谷科技有限公司

版本历史

版本/状态	作者	审核者	日期	修改记录
V1.0	仇金顺		2026.1	初版
V1.1	Emily Dong		2026.2	格式改动
V1.2	仇金顺		2026.5	增加 React 机制，Agent-skills-MCP 结构以及垂直类智能体更新

目 录

一、引言 5

1、背景与意义 5

2、白皮书的目的 5

3、适用范围 5

二、产品概述 6

1、产品定位 6

2、产品架构 7

3、产品优势 13

三、核心功能特性 18

1、增强检索（RAG） 18

2、全链路加密 19

3、RBAC 知识访问授权机制 19

4、知识库精细化授权管理 20

5、多端集成 20

6、垂直领域智能体 21

7、密文推理 22

8、多租户能力 22

9、安全审计 23

四、部署与实施 23

1、完全私有化部署（企业内网专属环境） 23

2、混合部署（本地应用 + 云端模型） 24

3、云端 SaaS 服务 25

4、云端全托管服务 25

五、成功案例 26

1、客户背景 26

2、核心需求 26

3、解决方案与产品应用 27

4、应用价值与客户认可 27

六、附录：发明专利 28

一、引言

1、背景与意义

在数字经济时代，企业知识资产已成为核心竞争力的关键组成部分。然而，当前企业知识管理普遍面临三大核心痛点：一是知识资产沉睡严重，分散存储于各类系统的文档、数据难以被高效检索与复用，导致业务响应效率低下；二是数据安全风险突出，内外部数据泄露事件频发，敏感知识资产缺乏全链路防护；三是合规压力持续增大，不同行业（尤其是金融、医疗、政府等领域）对数据隐私、权限管控、操作审计的监管要求日趋严格。

在此背景下，卫谷智 + 大模型应用产品应运而生。产品依托大模型核心能力与全链路安全防护技术，构建“对话咨询 + 精准找知识 + 业务对接落地”的企业核心需求闭环，全面解决企业业务系统转型与知识资产管理中的安全、效率、合规三大痛点问题，助力企业激活沉淀知识、降低运营成本、规避合规风险，为业务决策与可持续发展提供坚实支撑。

2、白皮书的目的

本白皮书旨在全面阐述卫谷智 + 大模型应用产品的技术架构、核心功能、安全体系、部署方案及合规能力，为企业用户、技术决策者、合作伙伴提供权威的技术参考，帮助相关方深入了解产品的技术优势与应用价值，为产品选型、部署实施及二次开发提供指导。

3、适用范围

本白皮书适用于对企业级知识管理、大模型应用落地、数据安全防护有需求的企业决策者、技术负责人、IT 运维人员，以及金融、医疗、政府、军工、电信、电力、制造、互联网等行业的潜在用户与合作伙伴。

二、产品概述

1、产品定位

1.1 产品定义

卫谷智+大模型应用产品是一款深度聚焦企业级场景的智能知识服务平台，依托先进大模型技术与成熟的企业服务架构，核心优势在于无需对企业现有业务流程进行颠覆性改造，最大程度降低企业落地成本与适配门槛。通过轻量化集成方案与高度灵活的配置功能，可快速嵌入企业现有 IT 体系，实现企业内分散知识资产的集中化安全管理、高效化复用流转与智能化场景应用。而数据传输、存储、处理过程中的加密安全有效地保证了企业独有知识和敏感信息聚集的安全。平台以企业知识安全为底线，以隐私保护为核心，以合规运营为准则，全面覆盖企业在知识全生命周期管理中的核心诉求，为不同行业、不同规模的企业提供一站式知识智能化解决方案，助力企业实现知识资产的价值转化与业务效能提升，解决了企业在人工智能领域“不敢用、不会用、用不起”的三大障碍。

1.2 产品优势

卫谷智 + 大模型应用产品是一款面向企业级场景的智能知识服务平台，依托大模型核心能力与全链路安全防护技术，构建 “对话咨询 + 精准找知识” 的双需求闭环，实现企业知识资产的安全管理与高效复用。

激活知识资产价值：打破企业内部各部门、各业务环节间的知识壁垒，破解知识分散存储、沉淀沉睡、传递不畅等痛点，通过智能检索、语义关联、内容聚合等能力，实现知识的快速定位、精准匹配与高效复用，显著缩短业务响应周期，提升员工工作效率与业务决策质量，让沉淀的知识资产成为驱动业务增长的核心动力。

构建全链路安全防护：建立覆盖知识资产从上传、存储、流转、使用到销毁的全生命周期安全防护体系，融合传输加密、存储加密、操作留痕、异常监测等多重技术手段，从源头阻断内外部数据泄露风险，严防敏感知识被未授权访问、篡改或扩散，确保企业知识资产的安全性与完整性。

满足精细化权限管控：深度适配企业组织架构与复杂业务场景，支持基于部门、岗位、角色、项目等多维度的权限划分，实现颗粒度可控的知识访问授权与操作权限管理。可根据业务需求灵活配置权限生效范围与有效期，既保障“合适的人获取合适的知识”，又防止知识越权访问，兼顾知识流通效率与管控安全性。

适配个性化业务场景：具备强大的多端集成能力，可无缝对接企业 OA、CRM、ERP、协同办公等现有系统。同时支持 ReAct 自主思考机制，可对复杂任务进行自主规划、推理与执行。依托业界主流的 Skills/Tools/MCP 智能体架构，能够快速搭建垂直行业专属智能体，可根据金融、医疗、制造、互联网等不同行业，以及小微企业、中型企业、大型集团等不同规模的个性化业务需求，灵活调整功能模块与服务模式，真正实现 “千人千面” 的场景化适配。

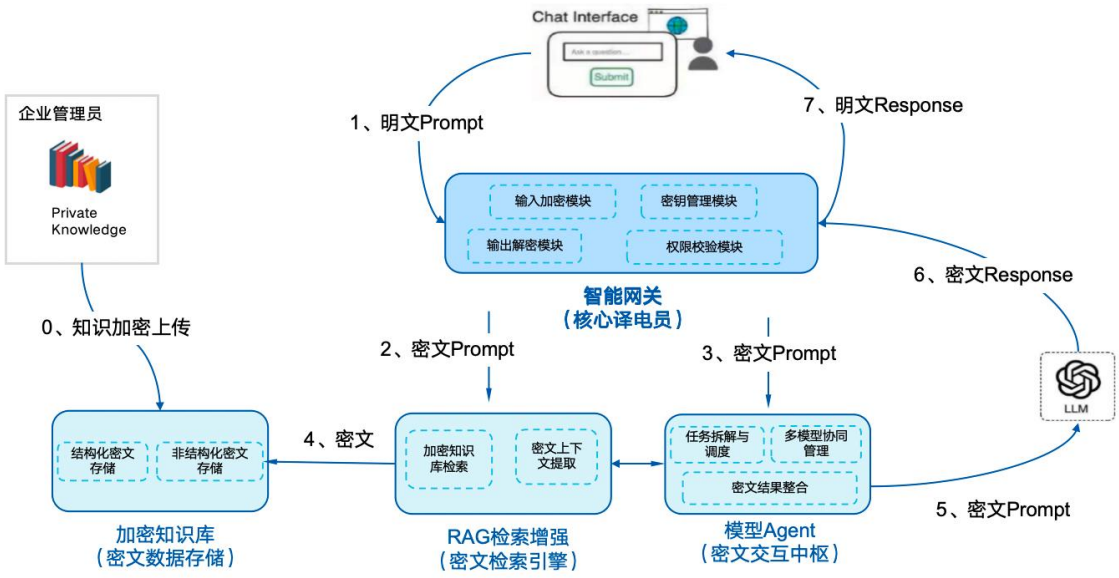
保障合规运营：内置完善的安全审计、隐私保护与合规管控功能，可实时记录知识全流程操作日志并支持追溯核查，针对敏感信息进行自动识别、脱敏处理，全面适配国家网络安全法、数据安全法、个人信息保护法等监管要求，同时满足各行业专属合规标准，助力企业实现合规化运营，规避合规风险。

2、产品架构

2.1 系统架构图

卫谷智+大模型应用产品采用分层协同架构设计，以安全可控为核心、以高效赋能为目标，通过四大核心模块联动构建闭环知识服务体系，全面支撑企业级知识资产的全生命周期管理与智能化应用。架构整体兼顾轻量化集成特性与高扩展性，可适配不同行业企业的 IT 环境与业务需求，在保障数据安全与合规的前提下，实现知识资产的价值最大化激活。各模块各司其职、协同联动，既实现了业务流程的无缝衔接，又通过技术手段筑牢安全防线，为企业提供稳定、高效、安全的智能知识服务支撑。

卫谷智+大模型应用整体架构如下图所示：



应用卫谷 AI 安全技术的完整构架

2.1.1 智能网关

智能网关作为架构的入口层核心模块，承担着统一接入、权限校验与流量管控的核心职责。支持多端设备与企业现有系统的无缝对接，通过标准化接口实现数据与请求的统一转发，无需改造企业原有业务流程即可快速集成。内置实时权限校验引擎，可基于企业组织架构与预设授权规则，对每一笔接入请求进行精准核验，拦截未授权访问。同时具备流量监控与限流熔断能力，可动态适配业务并发需求，保障系统运行稳定性，为后续知识流转与应用筑牢第一道安全与效率防线。

作为架构中的 “核心译电员”，其密码能力是全链路数据安全的核心支柱，构建起从输入到输出的密态防护闭环。在输入侧，输入加密模块对用户提交的明文 Prompt 执行实时加密，采用对称加密算法结合密钥管理模块下发的动态密钥，将明文转换为高安全性密文，确保用户指令在传输、检索与模型交互全流程中始终以密态存在，从源头阻断明文泄露风险。密钥管理模块是密码能力的 “信任中枢”，负责密钥全生命周期管理：基于密码学协议生成高强度密钥，结合业务场景动态分发密钥，并通过定期轮换、失效销毁机制规避静态密钥风险，为加密、解密操作提供可信的密钥支撑。在输出侧，输出解密模块接收大模型返回的密文 Response，从密钥管理模块获取对应密钥完成解密，将密文还原为用户可读的明文响应；解密前，权限校验模块会联动身份与权限体系，验证用户对该响应数据的访问权限，确保仅授权主体

可获取明文信息。这套密码能力与加密知识库、密态检索引擎深度联动，实现 “进必加密、出必解密、权必校验” 的安全逻辑，在不改变大模型原生交互流程的前提下，既保障企业私有知识的密态存储与使用，又确保大模型服务的可用性与安全性。

2.1.2 加密知识库

加密知识库是知识资产的安全存储与管理核心载体，采用分布式加密存储架构，对知识内容进行全生命周期加密保护。支持多种格式知识文档的集中存储与分类管理，可自动对上传知识进行格式解析与敏感信息识别，同步完成加密处理与安全备案。具备完善的知识版本管理与操作留痕功能，每一次知识的新增、编辑、删除均留存可追溯日志，结合分布式存储特性，确保知识资产的完整性与可用性，从存储层杜绝数据泄露与篡改风险，为知识安全提供核心保障。

2.1.3 RAG 增强检索

RAG 增强检索模块是提升知识复用效率的核心引擎，融合语义理解与精准检索技术，打破传统关键词检索的局限。通过对知识库内容进行语义分词、标签提取与关联建模，构建多维度知识索引体系，支持关键词、语义、上下文等多模式检索。依托大模型增强能力，可对检索结果进行智能优化与内容聚合，精准匹配用户业务需求，大幅缩短知识获取时间。同时具备检索结果溯源能力，明确标注知识来源与可信度，确保知识应用的准确性，高效激活沉淀知识资产价值。

2.1.4 模型 Agent

模型 Agent 作为架构的智能调度与应用核心，承担着大模型能力封装、业务场景适配与智能决策的职责。内置多场景适配引擎，可根据不同行业业务需求，定制化调用大模型能力，实现知识的智能问答、内容生成与业务辅助决策。具备灵活的智能体调度能力，可联动其他模块完成知识检索、安全校验、结果输出的全流程闭环。同时严格遵循合规要求，对大模型生成内容进行安全审核与敏感信息过滤，确保输出结果合规可控，为企业提供精准、安全的智能化知识服务。

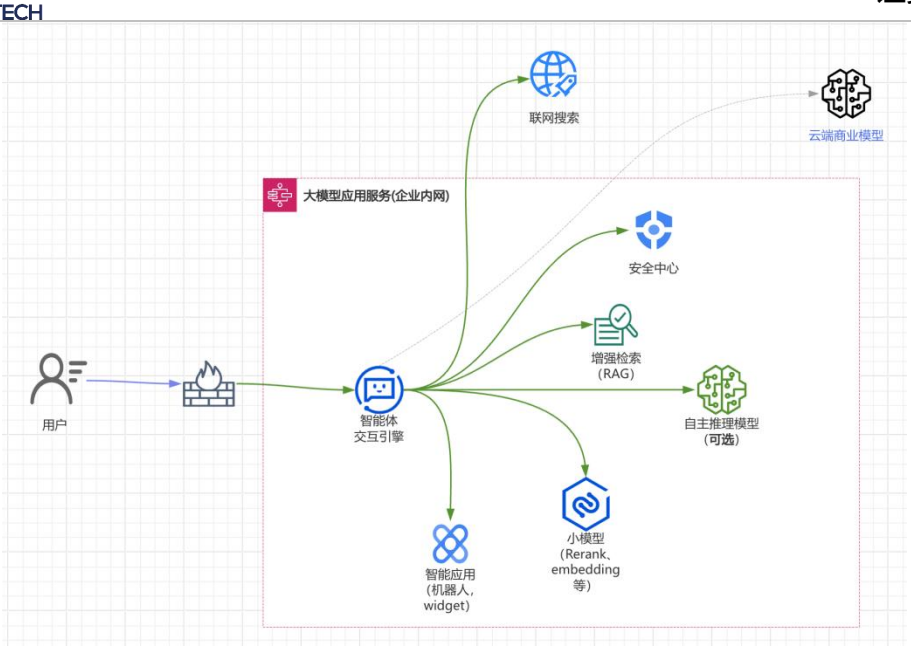
2.2 系统组成

本系统支持多形态部署模式：既可通过 SaaS 服务或云托管方式快速上线，也可根据企业合规与数据安全需求，采用驻场部署模式深度适配本地环境。以下以企业内网环境下的大模型应用部署为例，该方案以 “安全可控” 为核心设计原则，依托高度模块化的协同架构，为企业打造全链路闭环的一站式智能化业务支撑体系。用户请求通过企业防火墙完成安全接入后，由核心组件 “智能体交互引擎” 统一承接与调度。作为系统的神经中枢，该引擎可根据业务场景的差异化需求，动态联动各类功能模块，实现从请求解析、任务分发到结果生成与输出的全流程闭环管理，确保业务处理的高效性与安全性。

系统内置增强检索（RAG）模块，可深度关联企业内部知识资产，通过语义理解与精准检索实现沉淀知识的高效复用；小模型（embedding、Rerank 等）模块负责文本向量转换、结果重排序等基础算力支撑，为上层应用提供技术底座；智能体引擎支持业务流程的可视化配置与自动化执行，适配合同审核、客户跟进等多场景流程需求；安全中心则贯穿全链路，通过权限校验、内容审计与数据加密，保障企业信息安全与合规运营。

同时，系统具备灵活的扩展能力：智能应用模块可输出机器人、轻量化组件等场景化工具，直接嵌入企业现有业务系统；联网搜索功能可补充外部公开信息，增强回答的时效性与丰富度；可选配的自主推理模型则满足复杂业务场景下的深度逻辑推导需求，也可通过安全链路对接云端商业模型，进一步扩展大模型能力边界。

整体架构兼顾轻量化集成与高可扩展性，无需改造企业现有 IT 体系即可快速部署，在保障数据安全的同时，充分激活企业知识资产价值，助力各业务场景实现智能化升级。



- **智能体交互引擎**：采用业界领先的 Agent-Skills-MCP 分层智能体架构，以大模型为中枢、以技能化拆分为核心、以多智能体协同协议为纽带，构建可扩展、可复用、可快速落地的企业级智能体体系。该架构支持零代码 / 低代码快速构建行业智能体，无需重复开发即可快速适配金融、法务、财务、商旅等垂直场景，兼具技术先进性、业务灵活性与落地实用性，让企业 AI 能力随业务需求敏捷迭代、与时俱进。

- **增强检索（RAG）**：基于 RAG 技术构建的增强检索模块，为企业提供加密环境下的知识库全生命周期管理与精准检索能力，确保内部敏感数据全程安全可控，助力高效获取合规知识资源。

- **小模型**：集成多场景专用小模型，支持重排、文本嵌入与 OCR 识别等轻量化任务，无需依赖大模型即可实现高效处理，以低算力成本满足企业在内容理解、信息提取等场景的精准需求。

- **自主推理模型（可选）**:支持灵活部署模式，企业既可接入自有推理模型，也可选用云端商业模型，兼顾数据隐私与性能需求，为大模型应用提供稳定、可定制的推理算力支撑，适配不同规模企业的技术架构。

- **智能应用**：聚焦企业现有系统生态融合，提供企业微信机器人、Web Widget 等轻量化集成能力，无需重构原有系统即可快速接入 AI 能力，助力企业在日常办公场景中高效落地智能化应用。

- **安全中心**：作为大模型应用的原生安全防护核心，深度融合大模型场景下的安全需求与无感体验设计，整合「大模型加密引擎 + 精细化权限管控 + 全链路审计追溯」三大核心能力，提供覆盖企业文档、用户提示词、模型交互全场景的纵深安全防护，让安全贯穿业务全流程，用户操作全程无感无负担。

2.3 与其他企业系统的集成

智能应用模块是本大模型应用服务体系面向企业业务场景的轻量化输出端口，核心价值在于实现系统能力与企业现有业务系统的无缝融合。它以无侵入式集成方式，将大模型的智能问答、知识检索等能力封装为可快速嵌入的场景化工具，例如企业微信客服机器人、门户网站 Web 组件等，无需对企业现有 IT 架构与业务流程进行改造即可部署上线。通过这种方式，企业员工可在日常办公场景中直接调用智能服务，大幅降低智能化应用的使用门槛，同时依托系统底层的安全与管控能力，保障集成过程中的数据安全与合规性，助力企业各业务场景快速实现智能化升级。

- 多场景适配能力支持主流办公与业务系统的适配，包括即时通讯工具（如企业微信、飞书）、企业门户网站、OA 系统等。例如，在企业微信中部署智能客服机器人，员工可在会话中直接发起业务咨询；在门户网站嵌入 Web 组件，为外部客户提供 7×24 小时智能问答服务，覆盖内部办公与外部服务多场景。
- 标准化接口与轻量化部署提供 RESTful API、Webhook 等标准化接口，以及容器化部署包，企业仅需完成简单的接口配置与组件嵌入即可完成集成，部署周期可缩短至 0.5 个工作日。所有交互请求均通过智能网关统一转发，依托网关的流量管控与权限校验能力，保障集成后的系统稳定性与安全性。
- 安全与权限协同集成过程中严格遵循企业现有安全体系，通过与智能网关的权限引擎联动，实现对智能应用的访问权限管控。例如，仅允许特定部门员工使用企业微信机器人的敏感知识查询功能，同时所有交互数据均通过加密链路传输，依托加密知识库的全生命周期加密能力，杜绝数据泄露风险。
- 可定制化扩展支持根据企业业务需求定制功能模块，例如针对制造业的设备运维场景，可定制包含故障排查知识库的智能机器人；针对金融行业的客户服务场景，可定制具备合规话术校验的 Web 组件。同时可与 RAG 增强检索、模型 Agent 模块深度联动，实现检索能力与智能决策能力的场景化输出。
- 全链路可追溯所有通过智能应用发起的请求与交互内容，均会被安全中心记录并生成审计日志，支持事后追溯与合规核查，满足企业内部管理与行业监管的双重要求。

3、产品优势

3.1 以密文推理为核心的全链路安全防护

3.1.1 加密技术整体架构

卫谷智+大模型应用数据安全系统构建了 “端-网-云” 全栈协同的加密技术体系，以用户隐私与企业私有知识保护为核心，整合客户端加密、服务端加密、密钥分层管理、密文推理四大核心模块，形成覆盖数据 “采集-传输-存储-使用-共享-销毁” 全生命周期的密态防护屏障。系统依托 WG Crypto Client SDK 与 WG Crypto Server SDK 构建加密能力底座，通过三级密钥体系实现密钥的安全管控，以 Secure MetaData 实现权限与加密信息的绑定管理，最终通过密文推理技术突破 “数据使用与安全防护不可兼得”的行业痛点，实现“密态下运算、明文仅用户可见”的核心目标。

3.1.2 全栈加密组件技术支撑

3.1.2.1 客户端加密组件（WG Crypto Client SDK）

WG Crypto Client SDK 作为用户侧加密的核心载体，采用 WebAssembly 技术封装，适配 HTML5 前端架构，实现客户端轻量化、高性能加密运算。其核心功能包括三大模块：一是国密算法原生支持，内置 SM2（非对称加密）、SM3（哈希算法）、SM4（对称加密）等国密标准算法，覆盖数据加密、完整性校验、密钥交换等核心需求，确保加密方案符合国内安全合规要求；二是 Secure MetaData 全生命周期管理，支持生成包含工作密钥（DEK）、初始化向量（IV）、加密模式（ECB/CBC/CTR 等）、权限描述的安全元数据，并通过保护密钥（KEK）进行加密保护，防止权限信息与密钥泄露；三是保护密钥（KEK）协同管理，通过与 WG-DSCM 组件通信，从 KMS 安全获取企业级 KEK，确保密钥分发过程的安全性。

SDK 提供标准化接口适配多场景调用，其中 StreamEncryptor 类支持流式数据加密，通过 init-update-finish 三段式调用逻辑，实现大文件、流式数据的高效加密处理，并通过回调函数实时反馈加密进度与错误信息；CryptoClient 类则负责加密实例创建与密钥通信管理，依托浏览器 HTTP 通信能力与 WG-DSCM 协同，确保密钥获取与加密操作的原子性。WebAssembly 技术的应用使 SDK 突破

了前端语言的性能限制，加密运算效率较传统 JavaScript 实现提升 3-5 倍，同时保持跨浏览器、跨终端的兼容性。

3.1.2.2 服务端加密组件（WG Crypto Server SDK）

WG Crypto Server SDK 作为云端加密与解密的核心枢纽，采用 Node.js Addon 或 WebAssembly 封装，适配后端服务架构，实现与客户端加密体系的无缝协同。其核心能力包括加密 / 解密双向支撑、Secure MetaData 精细化管理、流式加解密三大模块：在加密算法层面，与客户端 SDK 同源支持国密算法族，确保端云加密逻辑一致性，同时提供解密算法实现密文数据的合规使用；在权限管控层面，通过 SecureMetaDataObject 类解析客户端传入的 Secure MetaData Cipher，支持用户 / 组权限的校验、添加、移除等操作，实现基于元数据的细粒度权限审计；在数据处理层面，提供 StreamEncryptor 与 StreamDecryptor 两类流式处理工具，分别用于文档结构化分段后的加密存储与密文数据的解密使用，适配 RAG 场景中文档分块处理的核心需求。

3.1.2.3 三级密钥体系

系统设计了 “主密钥（MK）- 保护密钥（KEK）- 工作密钥（DEK）” 三级密钥体系，通过密钥分层管理实现 “密钥泄露影响最小化” 目标，符合 NIST 等国际安全标准与国内密码管理规范：

主密钥（MK）：作为密钥体系的根密钥，采用非对称加密算法，全系统唯一且存储于 HSM（硬件安全模块）中，仅用于加密保护下级的 KEK，其生命周期长达数年，更换频率极低，通过物理隔离与逻辑防护确保绝对安全；

保护密钥（KEK）：作为企业级专属密钥，采用非对称加密算法，一个企业对应一个 KEK，其私钥经 MK 加密后存储于云端 KMS，公钥分发给企业管理员、经理等授权实体，仅用于加密保护 DEK，实现企业级数据隔离；

工作密钥（DEK）：作为数据加密的直接密钥，采用对称加密算法，为每个文档单独生成，加密后随密文文档一同存储，其生命周期与文档绑定，文档删除后 DEK 随之销毁，确保单个密钥泄露不影响其他文档安全。

三级密钥的流转遵循 “最小暴露” 原则：DEK 仅在加密 / 解密时短暂存在于内存，使用后立即清除；KEK 仅在 HSM 中解密并驻留于安全内存；MK 则完全隔离于业务系统，仅在 KEK 生成与轮换时调用，从根本上降低密钥泄露风险。

3.1.2.4 加密与权限的一体化载体

Secure MetaData 是系统实现 “加密保护与权限管控联动” 的核心技术，作为文档安全信息的载体，整合了工作密钥（DEK）、加密模式、权限描述等关键信息，通过 KEK 加密后与密文文档关联存储。其核心设计亮点包括：

一体化存储：将加密密钥与权限信息绑定，避免密钥与权限分离导致的安全漏洞，确保只有具备对应权限的用户才能通过解密 Secure MetaData 获取 DEK，进而解密文档；

多副本关联：一个文档可对应多个 Secure MetaData 副本，每个副本与文档所属的知识库关联，实现同一文档在不同知识库下的差异化权限管控，文档分配至新知识库时自动克隆元数据副本，取消分配时删除对应副本；

加密保护：采用 SM2 非对称加密算法对 Secure MetaData 进行加密，仅持有 KEK 私钥的系统组件可解密，确保元数据本身的安全性。

3.1.3 密文推理技术原理与实现

3.1.3.1 密文推理的核心定义与价值

密文推理是系统针对大模型推理阶段设计的核心安全技术，其核心逻辑是：通过无损加密技术将用户输入（Prompt）、企业私有知识等动态数据转化为密文，在大模型及中间处理节点（如 Retriever、智能体）中全程以密态形式流转与运算，仅当推理结果返回至用户侧时才解密还原为明文。该技术突破了传统

“明文推理 + 传输加密” 模式的安全瓶颈，从源头阻断数据泄露风险，实现 “大模型可用数据但不可见明文” 的目标，同时不影响大模型的推理准确性与运算效率。

需要明确的是，密文推理的保护范围聚焦于用户输入的动态数据与企业私有知识，不涉及大模型已训练完成的通用参数 —— 此类基础参数属于模型公共组件，具备通用性与共享性，不在密文保护范畴内，确保技术聚焦核心安全痛点。

*【技术注解】本章节涉及的核心技术已通过国家知识产权局审查并获得**发明专利授权**，其技术方案经权威机构审核认定具备独创性与行业领先性，受《中华人民共和国专利法》的排他性保护，相关专利证书详见附录，充分印证了本系统的技术壁垒与创新价值。*

3.1.3.2 密文推理的关键技术支撑

密文推理的实现依赖两大核心技术突破，确保密态数据可被大模型正常处理：

无损加密算法：采用对称加密算法，确保加密后的密文仍保留原始文本的分词特征，不破坏文本与 TokenID 的映射关系。例如，用户输入的含隐私信息的 Prompt 经加密后，仍可被大模型的 Tokenizer 拆解为有效语义单元，为后续推理奠定基础；

TokenID 精准映射：利用大模型 “通过 TokenID 识别语义” 的核心机制，确保密文分词后生成的 TokenIDs 与大模型 Vocabulary（Token 字典表）精准匹配。这一机制与大模型支持多语言的原理相通 —— 无论输入是明文还是密文，只要能映射到正确的 TokenID，模型即可完成理解与推理，实现 “密态推理不降级”。

3.1.3.3 加密技术核心优势总结

全链路密态防护：从用户输入到结果输出，动态数据全程加密，中间节点仅接触密文，彻底阻断泄露风险；

国密算法原生适配：全面支持 SM2/SM3/SM4 等国密标准，符合国内数据安全合规要求；

分层密钥隔离：三级密钥体系实现风险隔离，单个密钥泄露不影响整体安全，满足高安全等级需求；

密文推理创新：突破 “安全与效率对立” 瓶颈，在不降低推理性能的前提下实现隐私保护；

场景化适配：三类密文推理流程覆盖纯模型、RAG、联网搜索等核心场景，适配复杂业务需求。

3.2 以数据主权为核心的全周期管控

3.2.1 安全合规整体目标

卫谷智+大模型应用数据安全系统以 “用户隐私不泄露、企业知识不流失、全流程可追溯、合规要求全满足” 为核心目标，构建覆盖 “技术-管理-流程”的三维合规体系。系统聚焦大模型推理阶段的安全风险，针对用户输入（Prompt）隐私、企业 RAG 私有知识安全、智能体协同安全、合规安全四大核心场景，实现“用户侧端到端安全、企业侧知识可控、流程侧合规可审计”的三重保障，满足《网络安全法》《生成式人工智能服务管理暂行办法》《个人信息保护法》等国内法规。

3.2.2 核心安全合规目标拆解

3.2.2.1 用户输入（Prompt）隐私安全

核心目标是 “敏感信息进不去、拿不走、看不懂”，通过全链路加密与脱敏技术实现用户输入隐私保护：

加密保护：用户输入的文本、语音转文字等数据，在传输环节采用 TLS 1.3 强制加密，在暂存与处理环节采用端到端加密，防止传输窃听与服务器内存泄露；

权限管控：限制用户输入日志的访问权限，仅授权审计、运维角色通过多因素认证（MFA）查看，日志中不存储用户身份与输入内容的关联关系；

3.2.2.2 企业信息（RAG）安全

核心目标是 “私有知识可管、可控、可销毁”，构建分级防护与全周期管控体系：

访问边界隔离：对知识库按 “个人-公司”分级，按“全员-部门-项目级” 分类，结合用户身份与业务场景进行动态权限校验，例如 “财务文档仅财务岗在报销流程中可检索”；

数据加密：企业知识在客户端自动完成加密后再上传，确保传输，存储各个环节的安全加密保护；知识库数据采用 AES/SM4 加密，密钥由企业自主管理或 KMS 动态分配；

全周期管控：支持文档一键撤回与彻底销毁，服务器不保留任何企业数据，确保数据无法恢复。

3.2.2.3 智能体协同安全

核心目标是“跨智能体数据传输可追溯、授权可控”，解决多智能体协作中的数据泄露风险：

通信加密：Chat 智能体与文档智能体、垂直业务智能体等通过 MCP 协议通信时，采用 TLS 加密传输并添加消息签名，防止中间人篡改与伪造请求；

二次校验：跨智能体共享用户数据时，需经密文推理网关校验智能体权限，对高敏感数据进行加密降级或动态脱敏；

行为审计：日志自动标记 “跨智能体协作” 行为，记录调用方、被调用方、数据用途、处理策略，形成完整审计链。

3.2.3 安全合规核心优势总结

全生命周期覆盖：从数据上传到销毁，每个环节均有合规防护措施，无安全死角；

数据主权保障：企业自主掌控密钥与数据访问权限，支持数据随时撤回与彻底销毁，确保数据所有权不转移；

精细化权限管控：结合分级分类、动态授权、多因素认证，实现 “最小必要” 的权限分配；

安全审计：各类操作日志存证，满足合规审计与监管追溯要求；

三、核心功能特性

1、增强检索（RAG）

双需求闭环功能构建了“对话咨询”与“精准找知识”双向联动的知识服务体系，彻底打破传统知识服务中两种需求割裂的痛点，形成从需求发起至问题解决的完整服务链路。在自然语言对话咨询层面，产品搭载先进的语义理解模型，可精准识别用户口语化、场景化的业务疑问，支持上下文衔接、多轮交互，模拟人工咨询的沟通体验，快速响应基础业务咨询、流程查询等即时性需求，无需用户手动筛选知识。针对复杂、深度的知识需求，系统可自动触发精准检索功能，基于语义检索、关键词匹配、知识图谱关联等

技术，从海量知识库中定位核心知识资源，包括文档、案例、数据等，同时将检索结果转化为自然语言反馈给用户，实现“对话答疑—精准补全”的联动。

此外，双需求闭环并非单向服务，而是形成持续优化的循环机制。用户通过对话咨询产生的高频疑问，会自动沉淀为检索热点，优化检索算法的优先级；而检索过程中发现的知识缺口，也会反馈至对话模型的训练中，提升对话答疑的准确性。该功能大幅降低了用户获取知识的门槛，无论是一线员工的即时业务支撑，还是管理层的深度知识调研，都能通过高效交互获得满足，显著提升业务处理效率，避免知识获取过程中的重复劳动与信息遗漏。

2、全链路加密

全链路加密功能覆盖企业知识“上传—存储—检索—销毁”全生命周期，采用国家密码管理局认证的国密标准加密技术，构建全方位、高强度的知识资产安全防护体系，从源头杜绝知识泄露风险。在知识上传阶段，系统对传输数据采用 SM2 非对称加密算法进行加密处理，确保数据在传输过程中不被窃取、篡改，同时对上传文件进行完整性校验，防止恶意文件注入。存储环节采用 SM4 对称加密算法对知识内容进行加密存储，密钥由企业独立管控，结合分布式存储架构，实现加密数据的安全备份与容灾，即使存储设备被非法访问，也无法解析出有效知识内容。

在检索与销毁环节，加密机制持续生效：检索时采用按需临时解密，确保解密后的数据不落地，避免检索过程中的数据暴露；知识销毁采用安全擦除技术，彻底清除加密数据及密钥信息，同时留存销毁日志，确保销毁过程可追溯。相较于传统分段加密方式，全链路加密实现了“加密无死角、流转全安全”，完全适配金融、政务、军工等对数据安全要求极高的行业，为企业知识资产构建坚不可摧的安全屏障，保障知识在全流程中的合规流转与存储。

3、RBAC 知识访问授权机制

RBAC（基于角色的访问控制）知识访问授权机制以企业实际组织结构为核心，构建层级清晰、灵活适配的权限管理体系，实现权限分配与业务场景的深度融合。该机制摒弃传统粗放式的权限管理模式，将

权限与角色、岗位、部门进行强绑定，先根据企业组织架构划分部门层级，再按岗位职责定义角色类型，最后将知识访问权限批量分配至对应角色，形成“部门—角色—权限”的三级管控链路。例如，企业可为研发部门的核心研发岗分配知识库编辑、下载权限，为行政部门普通岗分配仅查看权限，确保不同岗位员工仅能访问与自身业务相关的知识资源。

同时，RBAC 机制支持权限的动态调整与继承，当员工岗位变动、部门调整时，系统可快速更新其角色权限，无需逐一配置，大幅降低权限管理成本。RBAC 机制从根本上解决了企业知识权限混乱、管理繁琐的问题，有效防范内部知识泄露，提升权限管理的规范性与高效性。

4、知识库精细化授权管理

知识库精细化授权管理在 RBAC 机制基础上，进一步细化权限管控颗粒度，支持按知识分类、访问范围等多维度定制授权规则，实现“千人千权”的精准权限管控。在知识分类维度，企业可按业务部门（如研发、销售、财务）、知识等级（如个人私有、企业共享）划分知识类别，针对不同类别配置独立授权规则，例如仅允许财务部门员工访问财务类机密知识。

访问范围维度支持按个人、部门、全企业、特定团队等圈层定义授权对象，同时可设置不同的访问权限，针对不同的授权对象设置管理权限、下载权限、仅查看等权限。此外，该功能支持授权规则的组合配置与批量管理，快速应用于不同业务场景，同时支持权限冲突检测，避免授权漏洞。知识库精细化授权管理满足了企业对知识资源的精准管控需求，尤其适用于知识类型复杂、岗位分工细致的大型企业，在保障知识安全的前提下，最大化实现知识的合理共享。

5、多端集成

多端集成功能提供全面的办公场景适配能力，通过 Web 企业门户、移动 App 与主流办公工具的深度对接，构建“桌面+移动”一体化的知识服务入口，满足企业员工多样化的办公需求。Web 集成可以在企业门户或者业务网站中集成智能助手，提供完整的知识库检索、对话咨询等核心功能。

移动 App 则聚焦移动办公需求，优化界面交互与操作流程，支持知识检索、对话咨询等核心功能，员工可在外出、出差等场景下随时获取知识支撑，提升工作灵活性。同时，产品支持企业微信机器人、钉钉、飞书等主流办公工具对接，通过机器人插件实现知识快速查询、业务流程触发等功能，员工无需切换应用即可在日常办公工具中享受知识服务。多端集成采用标准化 API 接口与适配协议，确保各端数据实时同步、功能一致，同时支持企业现有 IT 架构的无缝对接，无需大规模改造系统，降低集成成本。该功能打破了办公场景的时空限制，实现知识服务与日常办公的深度融合，提升整体办公效率。

6、垂直领域智能体

平台采用业界领先的 Agent-Skills-MCP 分层智能体架构，以大模型为中枢、以技能化拆分为核心。Agent 负责任务理解、规划调度与自主决策；Skills 将业务能力模块化、标准化，支持一键复用与灵活组合；MCP 实现智能体间安全通信、权限管控与数据协同。

垂直领域智能体能依托高精度文档识别技术，结合行业特性与企业业务需求，打造专属化、场景化的知识处理工作流，彻底解决企业业务场景适配性不足的问题。高精度文档识别技术支持 PDF、图片、扫描件等多种格式文档的精准解析，可自动提取文本、表格、图表等核心信息，实现文档内容的结构化处理，识别准确率达 99%以上，为业务工作流程落地提供坚实的数据基础。

在业务落地层面，产品面向金融、法律、商旅报销等领域提供开箱即用的垂直智能体。垂直智能体实现知识服务与业务流程深度绑定，显著减少人工干预，提升处理效率与标准化水平，全面满足专业场景的个性化与高可靠需求。

- **金融分析智能体**：实现知识归档 — 数据审核 — 报告生成全链路自动化，可解析多格式财务文档与合同文本，精准提取核心指标并完成数据校验。系统自动关联合规知识与风险规则，按模板生成专业分析报告，高效适配中小企业及上市公司财务分析需求。

- **法律咨询与合同审核智能体**：支持案例检索、法条查询与风险提示，可结构化解析合同文本，自动提取关键条款并识别法律风险。基于合规规则库给出专业审核意见与修改建议，帮助企业快速管控法律风险、提升法务处理效率。

- **商旅报销智能体**：商旅报销智能体支持行程归纳、发票精准识别、费用审核校验与报销单生成打印，通过 OCR 自动提取票据信息，完成验真、查重与合规检查。可无缝对接企业报销系统，实现流程自动化闭环，大幅降低人工成本，提升报销效率与体验。

7、密文推理

密文推理功能采用先进的密文计算技术，实现知识在密文状态下的模型推理运算，无需解密即可完成知识查询、分析与反馈，完美兼顾运算效率与数据安全。传统推理模式需先解密数据，存在解密过程中的数据泄露风险，且解密操作会占用大量系统资源，影响运算效率。密文推理则彻底规避这一问题，知识数据全程以密文形式存在，模型直接对密文数据进行推理运算，运算过程中不产生任何明文信息，从根本上杜绝数据泄露风险。

该功能采用优化的密文计算算法，在保障安全性的同时，将推理延迟控制在可接受范围，运算效率接近明文推理，满足企业实时查询、快速分析的业务需求。此外，密文推理支持多种推理场景，包括知识关联查询、趋势分析、智能推荐等，可广泛应用于敏感数据处理、核心知识分析等场景。例如，金融企业可基于密文推理分析客户敏感数据，生成个性化服务方案；政务部门可在密文状态下处理涉密知识，保障数据安全的同时完成业务办理。密文推理为企业提供了“安全与效率兼得”的知识处理方案，突破了传统加密技术对运算效率的限制。

8、多租户能力

多租户能力专为集团化企业、多分支机构场景设计，支持多组织、多部门独立使用系统，实现租户间数据隔离、资源独立分配，兼顾集团统一管理与各租户自主运营需求。该功能采用租户隔离架构，每个租户拥有独立的数据库、知识库与系统配置，租户间数据完全隔离，互不访问、互不干扰，确保各组织、部门的核心知识资产安全。例如，集团企业可为总部、各分公司、子公司分别创建独立租户，各租户可自主管理内部知识、配置权限规则、智能体启用，同时集团租户可获取各子租户的运营数据，实现统一监控与管理。

9、安全审计

安全审计功能全程记录知识全生命周期的各类操作行为，形成完整、不可篡改的行为日志，支持日志追溯、审计分析与合规报告生成，满足企业内部管控与外部合规监管要求。该功能覆盖知识操作、权限变更、系统访问、异常行为等全场景日志记录，包括知识的上传、下载、编辑、删除、分享等操作，权限的分配、修改、回收等变更行为，以及用户登录、退出、系统配置调整等访问记录，每一条日志均包含操作人、操作时间、操作内容、操作结果等关键信息，确保行为可追溯。

系统支持日志的多维度检索与筛选，管理员可按时间范围、操作人、操作类型、业务模块等条件快速定位目标日志，实现异常行为的快速排查。同时，安全审计功能提供智能化审计分析能力，可自动识别违规操作、异常访问、权限滥用等风险行为，触发实时预警，并生成多维度审计报告，包括操作合规报告、权限变更报告、风险分析报告等，为企业内部审计与外部监管检查提供有力支撑。安全审计功能构建了“事前预防、事中监控、事后追溯”的全流程安全管控体系，确保企业知识管理合规运营，规避合规风险。

四、部署与实施

1、完全私有化部署（企业内网专属环境）

目标客群：中大型企业、对数据安全与合规有高标准要求的组织

核心优势：数据完全在内网闭环流转，无外部泄露风险；提供敏感数据高级别防护；可支撑企业通过等保测评等安全合规审核。

基础资源配置要求：

模型计算资源（1 台）：部署基础各类专用模型（如嵌入模型、重排序模型、OCR 识别模型等）。建议配置为 8 核 CPU / 32GB 内存 / 16GB 显存。

应用平台资源（4 台）：部署集成了安全模块、知识库系统及企业级管理平台的“卫谷”大模型应用体系。建议每台配置为 4 核 CPU / 24GB 内存。

总计：约需本地资源 显存 16GB，CPU 24 核，内存 96GB。

配置说明：

基础配置可支持 1-3 路并发推理，满足初期业务试点与小规模场景使用；

如需提升并发性能（支持多用户同时使用）或启用全精度高性能模型（如完整版 Deepseek），可根据实际业务需求弹性扩容计算与存储资源。

可选模型范围：

通用大语言模型：DeepSeek、Kimi、DouBao、GPT 系列 (如私有化部署的 GPT-NeoX/LLaMA2-70B 等）。

专业领域模型：可根据企业业务需求定制（如金融、医疗、法律等行业专用模型）。

轻量化模型：支持量化版本（如 INT4/INT8）以降低资源占用。

核心参数要求：

模型尺寸：最低需支持 70B 参数规模的基础模型（可按厂商最低硬件配置自备）。

精度要求：最低支持 FP16 或 INT8 量化推理。

上下文长度：最低配置需支持 4K Token，可扩展至 32K（需调整资源配置）。

推理性能基准：首 Token 延迟：＜2 秒（FP16，70B 模型）。

2、混合部署（本地应用 + 云端模型）

目标客群：中小企业、对数据安全有要求且注重投入成本的组织

核心优势：兼顾经济性与安全性——企业数据本地加密存储，享有高级别安全防护；同时调用云端高性能模型服务，显著降低本地资源投入。

基础资源配置要求：

模型计算资源（1 台）：部署基础各类专用模型（如嵌入模型、重排序模型、OCR 识别模型等）。建议配置为 8 核 CPU / 32GB 内存 / 16GB 显存。

应用平台资源（4 台）：部署集成了安全模块、知识库系统及企业级管理平台的“卫谷”大模型应用体系。建议每台配置为 4 核 CPU / 16GB 内存

总计：约需本地资源 显存 16GB，CPU 24 核，内存 96GB。

配置说明：

基础配置支持 1-3 路并发推理，适用于业务试点与小规模应用场景；

推理模型部署于云端，可弹性调用高性能完整版模型（如全精度 Deepseek），以较小本地资源配置实现高效任务处理，大幅降低初期建设与运维成本。

根据使用需求弹性扩容“卫谷”大模型，满足高并发的使用需求。

若选择使用 128G 内存作为替代方案，其与 16G 显存在性能表现上差距不大，但能显著降低部署成本，更具性价比优势。

3、云端 SaaS 服务

目标客群：中小企业，特别是关注成本灵活性与运维便捷性的团队

核心优势：

弹性订阅：支持按月开通与暂停，实现轻量化起步与成本精确控制

数据安全：全链路加密存储，采用企业级数据防护机制，停用后支持彻底销毁客户数据

免部署运维：开箱即用，由卫谷提供一站式服务托管与技术保障

服务模式：所有服务由卫谷公司提供统一平台托管，客户通过授权访问登录即可使用“卫谷”大模型完整功能，为每个企业构建专属的智能应用空间。

4、云端全托管服务

目标客群：对数据主权有明确要求、已具备云资源的企业与机构

核心优势：

数据自主：客户数据完全储存在自有云服务器，保障数据主权与合规性

专业运维：由“卫谷”提供全程技术运维与模型更新服务，免除客户技术负担

弹性扩展：基于客户云环境灵活调配资源，支持业务平滑扩容

基础资源配置要求：

应用平台资源（4 台）：部署集成了安全模块、知识库系统及企业级管理平台的“卫谷”大模型应用体系。建议每台配置为 4 核 CPU / 16GB 内存

网络要求：稳定公网 IP，带宽≥10Mbps，支持 VPN 专线或加密通道接入

总计：约需云端资源 CPU16 核，内存 64GB。

配置说明：

基础配置可支持 1-3 路并发推理，满足初期业务试点与小规模场景使用；

如需提升并发性能（支持多用户同时使用）或启用全精度高性能模型（如完整版 Deepseek），可根据实际业务需求弹性扩容计算与存储资源。

服务模式：我方负责平台部署、模型更新、系统监控与故障处理和提供 7×24 小时运维监控与专业技术支持，企业数据全程存储于客户自有云环境，我方仅通过安全通道提供技术服务。

注：云端全托管服务也可以集群化部署：建立统一的 Weigullm 服务集群，通过独立容器为每位客户提供隔离服务。初始建设需要较高基础投入，但后续新增客户成本极低，且基础集群可按需弹性扩容。初步预估需要 8 台 4 核 16GB 内存的云服务器。

五、成功案例

1、客户背景

某股权投资基金合伙企业，作为集团旗下聚焦网络安全领域的专业投资机构，深耕产业链优质标的挖掘与价值评估，其核心业务环节涉及海量被投企业财务资料的处理、分析及投资分析报告生成。基于股权投资业务的特殊性，客户对财务数据的隐私安全、分析结果 的精准度及合规可追溯性均提出行业顶尖级要求，尤其强调核心财务信息在全流程处理中的安全隔离 与分析结论的决策参考价值。

2、核心需求

客户在传统投资分析流程中面临三大核心痛点：一是被投企业财务资料格式繁杂、数据维度多样，人工提取与整理效率低下，且易产生疏漏；二是财务数据属于核心敏感信息，需严格保障数据上传、存 储、

处理全链路安全，杜绝泄露风险；三是人工分析校验周期长，难以实现多维度数据交叉验证，报 告结论的一致性与准确性难以精准把控。为此，客户亟需一套兼具高安全性、精准数据分析能力与高 效报告生成能力的智能化解决方案，支撑投资决策效率与质量双提升。

3、解决方案与产品应用

针对客户核心诉求，我方为其部署定制化大模型应用产品，构建起“安全合规为底、精准分析为 核”的全流程投资分析闭环，各环节技术落地与功能实现如下： 数据安全层面，客户上传的各类财务资料（含财报、审计报告、流水凭证等）均经过全程加密处理后 存入专属知识库，搭配多层加密机制与精细化访问权限管控，仅授权人员可触发数据处理流程。同时，系统实时留存全链路操作日志，完整覆盖数据上传、存储、处理、调用全环节，严格满足金融行业审计追溯合规要求，从源头构筑敏感数据泄露的防护屏障。精准分析层面，产品依托优化训练的专业财务大模型，落地三大核心能力并形成逻辑闭环：其一为智能数据提取，可自动识别多格式财务资料中的营收、利润、资产负债率等核心指标，剔除冗余信息后生成标准化数据清单，提升数据预处理效率；其二为自动化校验分析，基于客户预设的数据规则对提取数据开展自动化核验，同步智能标记异常数据点，筑牢分析逻辑的准确性基础；其三为交互式交叉校验，在数据使用关键环节设置用户介入确认流程，通过人工复核与系统校验双向赋能，确保数据精准度，为后续报告生成提供可靠支撑。 报告生成层面，产品基于前述精准分析结果，自动生成结构化投资分析报告。系统支持客户自定义报告模板及核心指标展示维度，生成内容紧密贴合投资决策场景需求；同时保留灵活的人工修订接口， 既发挥智能化技术的效率优势，又兼顾专业人员的判断自主性，实现效率与精准度的双向平衡。

4、应用价值与客户认可

该产品的落地应用的实现了客户投资分析流程的智能化升级，核心价值体现在三大维度：其一，安全合规达标，产品完全满足客户对敏感财务数据的安全管控要求，全程无数据泄露风险，通过了客户内部网络安全合规检测，成为其核心业务场景的安全信赖载体；其二，分析精度领先，数据提取 准确率与报告结论一致性均达到 98%以上，交叉校验机制有效降低了人工误差，使分析结果可直接支 撑投资决策；其

三，效率显著提升，将原本需 3-5 个工作日的单份企业投资分析流程缩短至数小时，大幅释放分析师精力，聚焦核心决策环节。 凭借在数据安全与分析准确性上的突出表现，我方产品获得客户的高度认可，已成为其开展被投企业财务尽职调查、投资风险评估的核心工具，为其在网络安全领域的精准投资提供了坚实技术支撑。

六、附录：发明专利

证书号第8243577号

专利公告信息

发明专利证书

发明名称：一种字符加密方法、电子设备及计算机可读介质

专利权人：浙江网安卫谷科技有限公司

地址：310000 浙江省杭州市西湖区三墩镇振华路666号名栖首座6号楼603室

发明人：刘锦程;仇金顺

专利号：ZL 2025 1 0855009.9　　授权公告号：CN 120358014 B

专利申请日：2025年06月25日　　授权公告日：2025年09月09日

申请日时申请人：浙江网安卫谷科技有限公司

申请日时发明人：刘锦程;仇金顺

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，并予以公告。

专利权自授权公告之日起生效。专利权有效性及专利权人变更等法律信息以专利登记簿记载为准。

局长
申长雨

国家知识产权局

2025年09月09日

第 1 页 (共 1 页)

证书号第8236154号

专利公告信息

发明专利证书

发明名称：自然语言处理系统加密方法、电子设备及计算机可读介质

专利权人：浙江网安卫谷科技有限公司

地址：310000 浙江省杭州市西湖区三墩镇振华路666号名栖首座6号楼603室

发明人：刘锦程;仇金顺;洪新

专利号：ZL 2025 1 0855011.6　　授权公告号：CN 120378222 B

专利申请日：2025年06月25日　　授权公告日：2025年09月09日

申请日时申请人：浙江网安卫谷科技有限公司

申请日时发明人：刘锦程;仇金顺;洪新

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，并予以公告。

专利权自授权公告之日起生效。专利权有效性及专利权人变更等法律信息以专利登记簿记载为准。

局长
申长雨

国家知识产权局

2025年09月09日

第 1 页 (共 1 页)