



基于多源分析和多维特征融合的超高危漏洞AI预警系统研究

刘绪兴¹, 薛姍², 常玲², 赵延毫¹, 姚傲寒¹, 周犇¹, 雷培迪¹, 张晨²

(1. 中国移动集团设计院有限公司网络规划与设计优化研发武汉分中心, 湖北 武汉 430024;

2. 中国移动通信集团设计院有限公司网络规划与设计优化研发中心, 北京 100080)

摘要: 针对当前网络安全漏洞预警系统存在的数据“孤岛”、规则僵化与动态感知不足等局限性, 提出一种基于多源数据融合与AI辅助多维评分的智能研判系统。现有技术依赖单一漏洞库(如CNNVD/NVD), 导致漏洞信息不完整; CVSS等静态评分规则难以适配新型攻击特征, 传统机器学习模型缺乏语义关联分析能力; 同时, 忽视网络热度追踪致使高危漏洞预警滞后。本系统通过三阶段创新设计突破上述瓶颈: 一是提出多源异构数据融合构建补全机制, 二是提出基于AI辅助的语义分析与动态评分, 三是引入热度模块实时感知网络热度。通过加权动态研判, 系统实现对超高危漏洞的精准识别。实验表明, 该系统显著降低了误报率与漏判风险, 响应效率提升明显, 为关键基础设施的主动防御提供了技术支撑。

关键词: 超高危漏洞识别; 多源数据融合; AI辅助评分; 网络热度追踪; 漏洞预警系统

中图分类号: TN918

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2025282

0 引言

随着网络安全威胁日益复杂化和数字化转型加速, 漏洞攻击呈现规模化、隐蔽化趋势, 传统依赖单一漏洞库和静态评分规则的预警模式难以满足新型高危漏洞的快速识别需求。现有漏洞预警系统通常基于单一数据源采集漏洞信息, 导致漏洞研判字段缺失和高危漏洞数据覆盖面受限。针对现有技术的数据碎片化、研判规则固化、研判滞后性及语义理解缺失等问题, 本文提出一种融合规则、AI大模型与网络热度的三重加权预警机制, 旨在提升漏洞响应的精准性与时效性。通过整合多漏洞库并利用AI大模型进行深度语义分析, 本方法实现了对漏洞上下文的关联感知; 结

合网络热度追踪与时间衰减模型, 构建了动态评分与阈值判定机制。实验表明, 该系统能显著提升超高危漏洞识别的准确性与时效性, 为构建主动防御体系提供了有效解决方案。

1 现有方案与技术原理阐述

当前网络安全漏洞预警系统存在多方面的局限性。首先, 现有技术多依赖单一漏洞库, 比如从CNNVD或NVD漏洞库获取数据, 缺乏跨平台信息整合能力, 导致漏洞描述、利用字段及影响范围等信息不完整^[1]。其次, CVSS评分系统等规则引擎采用静态权重, 难以动态适配新型漏洞攻击特征^[2], 且传统机器学习模型仅用于基础分类^[3], 未能充分利用AI大模型的语义理解能力,



导致漏洞上下文关联分析薄弱。此外，现有系统普遍忽略网络热度数据的实时追踪，仅依赖漏洞发布时间或库内等级评判，无法及时识别突发性高危漏洞，造成预警滞后。数据“孤岛”、规则僵化与动态感知不足等问题进一步加剧了误报率和漏判风险。

本文提出一种基于多源数据融合与AI辅助多维评分的智能研判系统，旨在解决上述核心问题：通过整合CNNVD、NVD、阿里云等漏洞库信息，构建跨平台字段补全机制，弥补漏洞利用方式、影响范围等关键信息的缺失；结合DeepSeek等AI大模型对漏洞描述文本进行语义级分析，关联攻击路径与上下文影响，动态生成辅助评分，突破传统规则引擎的静态权重限制；同时引入网络热度追踪模块和时间衰减模型，实时捕捉漏洞讨论热度，优化风险评估时效性。最终通过加权规则研判、AI辅助打分及热度值计算，形成动态阈值判定机制，显著提升超高危漏洞识别的准确性与响应效率，满足企业关键基础设施的主动防御需求。

2 系统设计

2.1 系统模块组成与功能介绍

AI智能研判超高危漏洞预警系统可立即执行巡检任务或按照周度或日度开展定时巡检任务来实时监控超高危漏洞风险，其主要包括数据采集层、数据处理层、智能分析层、研判决策层和应用层5层结构。各层通过标准化数据接口交互，完整清晰地展示了从多源数据采集到多维数据研判直到最终预警的闭环全流程工作结构。

AI智能研判超高危漏洞预警系统架构如图1所示，包含数据采集层、数据处理层、智能分析层、研判决策层和应用层5层结构。数据采集层是漏洞信息入口层，主要用于爬取漏洞数据和网络热度信息，构建漏洞信息基础池，突破单源数据覆盖局限。数据处理层是漏洞整合枢纽层，主要用于补全漏洞字段和建立黑白名单机制进行数

据清洗，消除数据“孤岛”，建立基于跨库映射规则的标准化漏洞画像。智能分析层是漏洞决策的核心层，主要用于规则评分、AI评分以及热度值计算，量化漏洞风险以支撑动态研判。研判决策层是漏洞风险评估的关键判定中枢，主要用于多维加权算法计算漏洞风险评分，可以动态调整加权比重，引入热度分值计算实时影响力，精准判定超高危漏洞，触发预警逻辑。应用层主要处理前端可视交互，通过可视化看板展示漏洞详情与预警进度，集成自动化工单系统并闭环追踪，实现漏洞全生命周期管理。接下来按层次对主要模块进行详细说明。

2.1.1 数据采集层

数据采集层主要模块如图2所示，负责漏洞数据和热度数据的入库采集，对采集流程的发起立即执行任务或定时执行管理任务，主要包括爬虫集群模块、配置管理模块（中心）、对外接口模块和热度采集模块。其中，爬虫集群模块用于爬取CNNVD国家漏洞库数据作为原始漏洞数据；配置管理模块用于爬取信息配置管理、多源数据库映射规则库管理以及对外连接配置等相关配置；对外接口模块主要用于爬取第三方漏洞数据，包括NVD漏洞库和阿里云漏洞库数据；热度采集模块主要用于漏洞CVE编号搜索引擎热度抓取管理。

2.1.2 数据处理层

数据处理层的主要模块如图3所示，负责对漏洞数据进行清洗、对齐与补全，支持黑白名单设置过滤出高危漏洞库，主要包含数据清洗模块、数据补全模块、黑白名单配置模块，由配置管理中心统一管理规则和策略。其中，数据清洗模块主要用于原始漏洞数据去噪与结构化；数据补全模块主要用于跨漏洞库字段关联与缺失信息修复；黑白名单配置模块主要用于漏洞过滤与优先级控制。配置管理中心统一进行映射规则管理、过滤策略管理和存储策略管理。

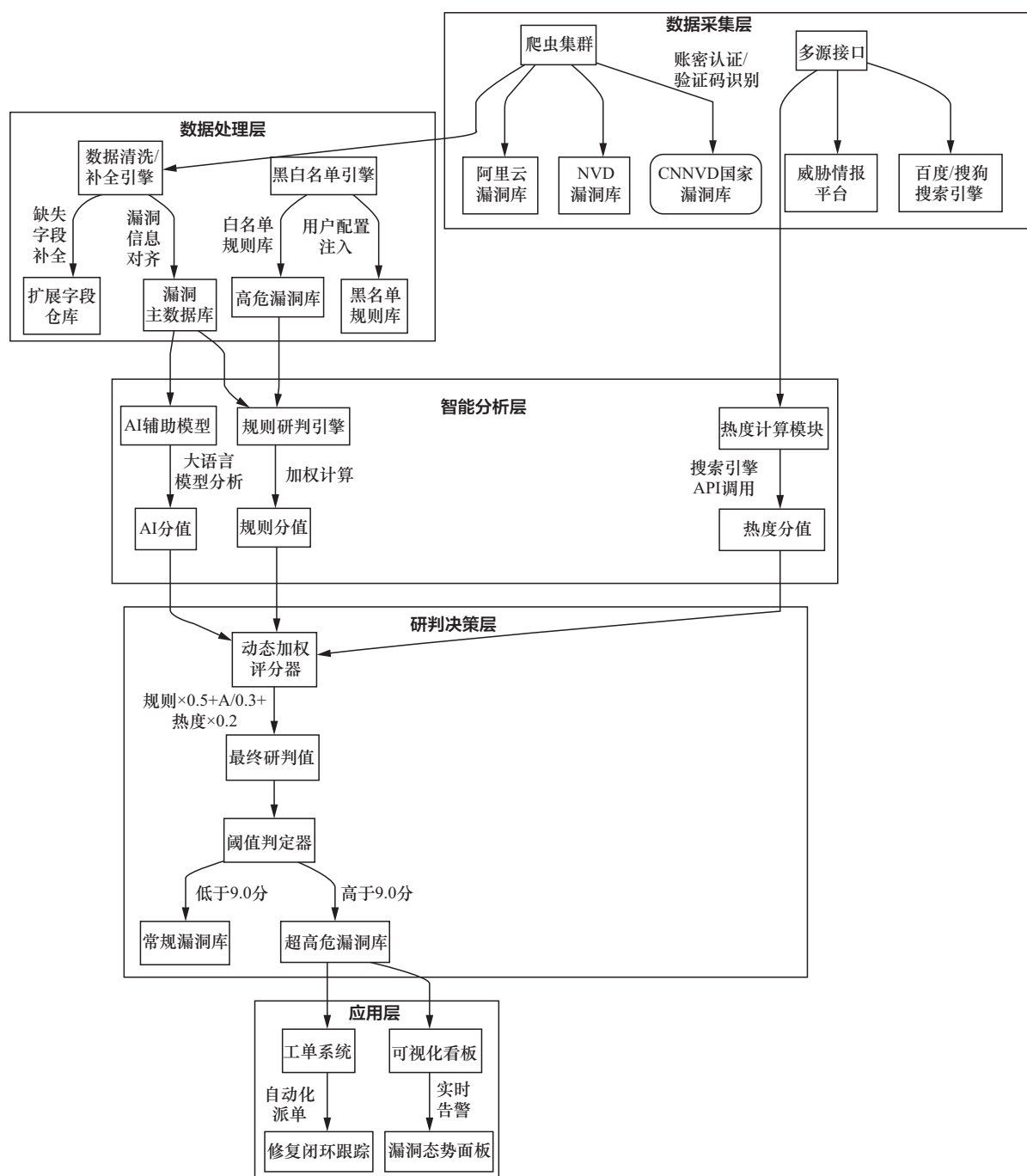


图1 AI智能研判超高危漏洞预警系统架构

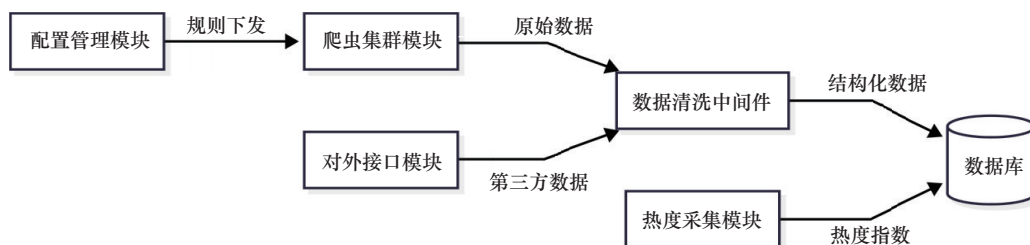


图2 数据采集层主要模块

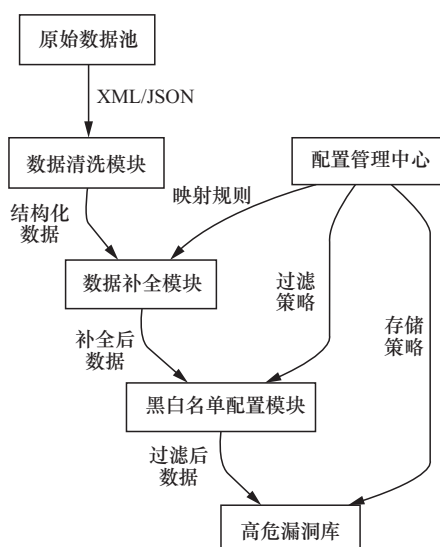


图3 数据处理层的主要模块

2.1.3 智能分析层和研判决策层

智能分析层&研判决策层的主要模块如图4所示，负责对漏洞进行研判分析打分，按照设定阈值进行判定进入预警流程，主要包含规则研判模块、AI辅助研判模块、热度追踪模块以及加权融合引擎模块。其中，规则研判模块主要基于《信息安全技术安全漏洞等级划分》（GB/T30279-2013）体系扩展的漏洞风险量化规则评分；AI辅助研判模块主要用于语义级漏洞特征提取与AI大模型动态评分；热度追踪模块主要用于网络讨论热度实时量化与风险评估；加权融合引擎模块主要用于多维评分动态融合与阈值判定。

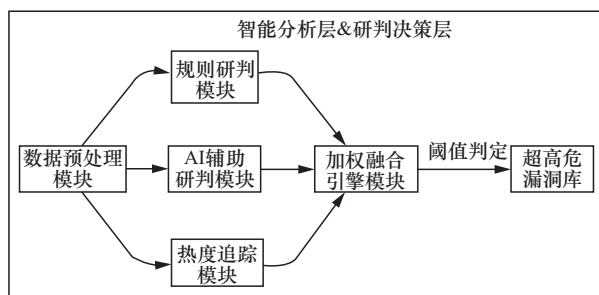


图4 智能分析层&研判决策层的主要模块

2.1.4 数据应用层

AI智能研判超高危漏洞预警系统的数据应用层主要负责前端可视化展示高危漏洞报告和预警

可视化面板，支持多维度联合查询。集成工单系统追踪漏洞从预警到复测的工单系统全流程管理。基于多用户的权限管理模块支持批量导出各种自定义报表等功能。

2.2 AI智能研判超高危漏洞预警系统关键技术和流程

本系统主要采用多源数据采集和多维研判评分的技术方案，用于超高危漏洞风险预警处理。系统采用分层结构设计，包括数据采集层、数据处理层、智能分析层、研判决策层和数据应用层5层结构。各层结构独立并协同运行工作，实现高效的超高危漏洞预警处理流程。为了提高系统的并发处理能力，采用多线程和异步的编程技术，确保能够快速处理大批量爬虫或研判任务。另外，考虑到系统的可扩展性，通过配置中心机制允许用户根据需求扩展功能，如新增爬虫规则、更改黑白名单等。本文的核心技术是通过多源数据采集与结合跨源字段映射规则实现字段信息补全来获取漏洞数据库信息，然后采用正则表达式匹配黑白名单实现筛选过滤，引入AI大模型解析提取语义特征来实现辅助评分，抓取搜狗等搜索引擎搜索统计关键词热度频次信息，引入网络热度值来提高高危漏洞的实时报警率，然后通过多维加权评分模型来获取最终的研判分值，按阈值判定是否为超高危漏洞，并且形成预警工单完成漏洞预警闭环处理。

2.2.1 预警研判算法

预警研判算法是本系统最核心的关键技术，主要由规则研判算法、AI研判模型、热度研判算法和多维加权研判算法组成。

（1）规则研判算法

基于漏洞风险评估的预警需求，本算法综合CVSS评分框架并引入动态加权机制，结合漏洞涉及的风险评估字段（风险等级、访问路径等）构建多维度量化模型。以下是核心模块与算法实现。

1) 风险评估字段定义与分类分级量化标准

对每个研判评估字段进行等级划分, 并且赋予量化基准分值, 通过量化评分, 为后续规则研判算法提供数据输入。

2) 动态规则研判加权公式设计

由于漏洞风险评估字段的多样性, 设计选择加权分配算法来计算规则研判分值, 另外考虑漏洞利用链的实战影响, 权重系数按照专家人工研判设置并可以动态调整, 动态规则研判加权计算式如下:

$$\text{TotalScore} = \sum_{i=1}^n (w_i \times s_i) + \text{BonusAdjustment} \quad (1)$$

其中, TotalScore 为规则研判分值, w 为权重系数, s 为等级量化评分值, 另外添加附加调整项 BonusAdjustment 。经过专家研判确认, 对权重系数设置默认值, 风险等级和影响范围设置权重为 0.25, 访问路径设置权重为 0.2, 权限需要和攻击复杂度设置权重为 0.15。附加项则为用户交互和存在 POC 的量化分值。根据规则研判的结果, 可以形成漏洞预警研判的初步结论。若规则研判值大于 15 的研判阈值, 则定为高危预警漏洞。为下一步多维研判创造可选条件。这种规则加权评分算法可以有效避免传统 CVSS 的静态评分偏差。量化 POC 存在性和用户交互需求, 更贴近实际攻击场景。结合关键基础设施保护需求, 提升高危漏洞优先级。本算法通过多字段量化、动态权重分配及阈值自适应优化, 实现了对高危漏洞风险的精准研判。

(2) AI 研判模型&热度研判算法

1) AI 研判模型

为了优化规则研判算法, 提高漏洞关联性分析研判, 引入 AI 大模型进行研判, 专注于进行漏洞语义解析、知识推理与动态优化。采用 DeepSeek 等推理模型提取漏洞描述文本中的上下文语义特征, 结合大模型本身漏洞专业知识和企业知识, 支持并行处理长序列输入, 对漏洞信息深入

关联分析研判。AI 研判的计算式如下:

$$\text{AIScore} = \text{deepseek}(\text{TEXT}, \text{Prompt}, \text{Beta}) \quad (2)$$

其中, TEXT 表示漏洞描述介绍文本; Beta 表示 AI 模型输入的参数控制, 比如控制生成随机性、生成长度、上下文记忆设置等相关参数; Prompt 为调用 AI 大模型的提示词, 其设置需要满足对 AI 评分的所有要求。本研判模型为专业 AI 评分模型, 要求精准提取出漏洞描述中包含的攻击路径、权限需求、影响范围等关键结构化特征, 要求对漏洞进行推理分析展示预测潜在利用场景, 漏洞是否关联供应链攻击等相关信息, 同时结合此漏洞对企业可能产生的影响范围和大小进行分析, 最终给出 AI 研判分值, 并且限定 AI 评分的范围为 0~10 分。

2) 热度研判模型

热度研判模型是智能漏洞预警系统的核心模块之一, 通过量化网络讨论热度、威胁情报传播强度及时效性, 实现对漏洞风险的动态感知。引入指数衰减函数动态调整历史数据的权重, 热度衰减计算式如下:

$$\text{Search Heat}_t = \sum_{k=1}^n \frac{\text{KeywordCount}_k}{1 + e^{-\alpha(t_{\text{current}} - t_k)}} \quad (3)$$

其中, α 表示衰减系数, 默认设置为 0.1, 表示 24 小时后权重下降 50%。 t_k 表示关键词第 k 次出现的时间戳。采用分段优化思路, 短期爆发期 (<24 小时): 线性衰减保留 80%~100% 权重; 中期传播期 (24~72 小时): 指数衰减保留 30%~80% 权重; 长期消退期 (>72 小时): 对数衰减保留 5%~30% 权重。

接下来, 设置最大热度值和最小热度值用于归一化当前的搜索热度值。最大热度值计算式如下:

$$\text{MaxHeat} = \max(\text{KeywordCount}_k^{\text{history}}) \times \beta \quad (4)$$

其中, $\text{KeywordCount}_k^{\text{history}}$ 表示关键词在历史时间段内的搜索频次集合; β 表示动态调整系数, 默



认设置为1.0,可根据突发场景适应性放大(如检测到0day漏洞时, α 可提升至1.2)。最小热度值计算式如下:

$$\text{MinHeat} = \mu_{\text{baseline}} + \beta \times \sigma_{\text{baseline}} \quad (5)$$

其中, μ_{baseline} 为正常时期(如无漏洞披露时)搜索频次的均值, σ_{baseline} 为标准差, β 为动态调整置信系数,一般取1.0。最后通过MaxHeat和MinHeat对原始热度值进行归一化。归一化热度值计算式如下:

$$\text{NormalizedScore} = 10 \times \frac{\text{SearchHeat} - \text{MinHeat}}{\text{MaxHeat} - \text{MinHeat}} \quad (6)$$

通过归一化公式,消除多源数据量纲差异,统一输出为0~10分;使用动态反馈机制,当MaxHeat或MinHeat更新时,历史归一化结果需重新计算以保证一致性。

(3) 多维加权研判算法

基于CVSS评分、攻击路径复杂度等确定性指标的规则模型稳定性高但灵活性不足,难以覆盖复杂语义场景。AI评分模型擅长语义推理与上下文关联,但对数据质量敏感,低置信度时易产生误判。热度模型反映实时舆情动态,但易受无关噪声干扰。因此考虑多维因素设计加权研判算法,通过动态分配权重,发挥各模型优势,弥补单一模型的局限性。多维加权研判算法基本计算式如下:

$$S_{\text{final}} = w_{\text{rule}} \cdot S_{\text{rule}} + w_{\text{ai}} \cdot S_{\text{ai}} + w_{\text{heat}} \cdot S_{\text{heat}} \quad (7)$$

其中, w 为各模型的权重且三者权重和约束为1, S 为各模型的归一化得分,范围是0~10。考虑AI研判模型存在不确定性以及难解释性,特设计动态调整权重策略,通过设置AI置信度来补偿规则评分进行权重动态调整。若AI置信度 $\text{Conf}_{\text{ai}} < 0.7$,则触发规则补偿:

$$w'_{\text{rule}} = w_{\text{rule}} + (1 - \text{Conf}_{\text{ai}}) \cdot w_{\text{ai}} \quad (8)$$

其中, w' 为动态调整后的规则权重,然后进行归一化来统一各模型权重:

$$w_i = \frac{w'_i}{w'_{\text{rule}} + w'_{\text{ai}} + w_{\text{heat}}} \quad (9)$$

通过权重初始化,确保默认状态下三方模型均衡参与决策,当AI模型置信度不足时,降低其权重并增强规则模型的补偿作用,减少误报风险,最后强制权重总和为1,保证评分范围可控。多维加权研判算法伪代码见算法1。

算法1 多维加权研判算法

输入 3个研判模型的评分值 $S=[S_{\text{rule}}, S_{\text{ai}}, S_{\text{heat}}]$ 、默认权重 $W=[W_{\text{rule}}, W_{\text{ai}}, W_{\text{heat}}]$ 和AI置信度 Conf_{ai}

输出 加权评分值 S_{final}

初始权重分配(可配置)

$w_{\text{rule}} = 0.4$

$w_{\text{ai}} = 0.3$

$w_{\text{heat}} = 0.3$

AI置信度补偿机制

if $\text{Conf}_{\text{ai}} < 0.7$:

$\text{delta} = (1 - \text{Conf}_{\text{ai}}) \times w_{\text{ai}}$

$w_{\text{rule_adj}} = w_{\text{rule}} + \text{delta}$

$w_{\text{ai_adj}} = w_{\text{ai}} \times \text{Conf}_{\text{ai}}$

else:

$w_{\text{rule_adj}} = w_{\text{rule}}$

$w_{\text{ai_adj}} = w_{\text{ai}}$

权重归一化

$\text{total} = w_{\text{rule_adj}} + w_{\text{ai_adj}} + w_{\text{heat}}$

$w_{\text{rule_final}} = w_{\text{rule_adj}} / \text{total}$

$w_{\text{ai_final}} = w_{\text{ai_adj}} / \text{total}$

$w_{\text{heat_final}} = w_{\text{heat}} / \text{total}$

综合评分计算

$S_{\text{final}} = w_{\text{rule_final}} \times S_{\text{rule}} + w_{\text{ai_final}} \times S_{\text{ai}} + w_{\text{heat_final}} \times S_{\text{heat}}$

return S_{final}

3 实验方案与结果讨论

本节将详细阐述实验环境、数据集的构建与

预处理、核心模块的实现细节、性能评估指标、对比基线模型，并通过量化数据与案例分析，系统性地验证本文提出的系统的有效性与先进性。

3.1 实验方案

为确保实验结果的科学性和可复现性，本文设计以下实验方案，旨在从数据、模型、流程和评估等多个维度，对智能研判系统进行全面验证。

3.1.1 实验环境与工具

本实验在一台配置了高性能GPU的服务器上运行，操作系统为Windows。主要软件环境：编程语言为Python3.10，数据处理与分析库为Pandas、Numpy等工具，深度学习与大模型框架有OpenAI、Hugging Face等，数据库PostgreSQL用于存储和管理各种漏洞数据。数据采集工具为自主开发的网络爬虫程序，包含aiohttp和requests包的核心请求模块、beautifulsoup4和lxml等相关解析模块、ddddocr等强大的验证码识别工具等，用于从各大漏洞库和信息源获取数据。

3.1.2 实验数据集构建与预处理

构建一个高质量、多来源的综合漏洞数据集是本文的基石，也是验证多源数据融合有效性的前提。为了克服单一数据源导致的信息“孤岛”问题，本文从以下多个权威和公开渠道采集了2020—2025年的漏洞数据，共计约16万条原始记录。CNNVD作为国家级漏洞库，提供了大量与国内软硬件相关的漏洞信息，其独特的漏洞编号、中文描述和风险等级为本系统提供了重要的补充视角。NVD作为全球最权威的漏洞数据库之一，提供了CVE ID、CVSS评分、CWE分类、CPE信息及详细描述等标准化数据，本文通过其官方数据接口下载JSON格式的完整数据。阿里云漏洞库是国内比较专业的企业级漏洞库，通过监控其漏洞库获取与漏洞利用等相关信息，为语义分析提供深层技术背景。

原始数据异构性强、信息缺失普遍，必须经过严格的预处理流程。首先，对从各来源获取的

数据进行解析，将JSON、XML、HTML等不同格式的数据统一转换为结构化的扁平格式。此过程包括去除无关标签、处理编码问题和标准化日期格式。以CVE ID为核心关联键，将来自NVD、CNNVD及阿里云的同一漏洞信息进行匹配和对齐。对于部分CNNVD漏洞无对应CVE ID的情况，本文采用基于漏洞标题、涉及厂商和产品名称的模糊匹配算法进行关联。经过上述步骤，构建了一个多源融合增强漏洞知识库，显著提升了漏洞信息的完整性和准确性。

3.1.3 实验性能评估指标

为了全面、客观地评估本系统的性能，本文采用分类任务中广泛使用的标准评估指标^[4]。笔者将漏洞研判任务定义为一个二分类问题：将漏洞划分为超高危和非超高危。

精确率 (Precision)： $Precision = TP / (TP + FP)$ ，衡量在被系统判定为超高危的漏洞中，真正是超高危的比例。高精确率意味着低误报。

召回率 (Recall)： $Recall = TP / (TP + FN)$ ，衡量在所有真实超高危漏洞中，被系统成功识别出的比例。高召回率意味着低漏判。

F1分数： $F1 = 2 \times (Precision \times Recall) / (Precision + Recall)$ ，精确率和召回率的调和平均值，是综合评价模型性能的重要指标。

误报率 (false positive rate, FPR)： $FPR = FP / (FP + TN)$ ，衡量在所有真实非超高危漏洞中，被系统错误判断为超高危的比例。此指标直接关系到安全运营团队的无效工作量。

漏报率 (false negative rate, FNR)： $FNR = FN / (FN + TP)$ ，衡量在所有真实超高危漏洞中，被系统遗漏的比例。这是衡量预警系统性能最关键的指标之一，直接关系到潜在的安全风险。

3.1.4 实验对比基线模型

为了验证本系统各创新模块的有效性，本文设立了以下3个基线模型进行对比。

基线模型1：模拟当前最常见的漏洞预警方



式。仅使用NVD单一数据源，并完全依赖其提供的CVSSv3.1基础分进行排序和阈值判断（如分数>9.0即超高危）。

基线模型 2：该模型使用笔者构建的“多源融合增强漏洞知识库”，但评判规则依然仅依赖CVSSv3.1评分。此模型用于独立验证多源数据融合带来的信息增益是否能间接影响风险判断（如更精确的CPE可能导致环境评分变化）。

基线模型 3：该模型在融合数据的基础上，使用传统机器学习方法代替大模型进行语义分析。本文对漏洞描述文本进行TF-IDF特征提取，并训练一个随机森林分类器来预测其风险等级。此模型用于对比AI大模型与传统NLP方法在语义理解深度上的差异。

本文系统：集成了多源数据融合、基于DeepSeek大模型的AI辅助评分以及网络热度追踪的完整系统。

3.2 结果分析

本节将展示并分析各项实验的结果，以验证本文系统的综合性能。

3.2.1 多源数据融合有效性验证

本节首先量化数据融合对信息完整性的提升效果。在笔者构建的数据集中随机抽取10 000个漏洞样本进行统计，结果见表1。

表1 数据融合前后关键字段完整度对比

关键字段	NVD单一数据源完整度	多源融合后完整度	提升率
中文描述	0%	85.2%	—
漏洞利用 代码(PoC)信息	12.5%	48.7%	+289.6%
精确的受影响 组件版本	65.3%	92.1%	+41.0%
官方修复方案链接	70.1%	95.8%	+36.7%

从表1可以看出，经过多源数据融合与字段补全，漏洞信息的完整性得到了很大的提升。特别是对于漏洞利用代码信息这类直接关系到漏洞实际威胁程度的关键情报，完整度提升了近3倍。

这为后续的AI语义分析和精准研判提供了高质量的基础条件，从根本上解决了因信息缺失导致的研判困难。

3.2.2 AI辅助语义分析与动态评分性能评估

在AI辅助评分模块中，笔者选用了DeepSeek-V2模型^[5]。选择该模型的原因在于其强大的语言理解能力、高效的推理性能以及通过MoE（mixture-of-experts）架构实现的成本效益。实现方式如下：设计一套包含漏洞利用复杂性、攻击路径、数据泄露风险、业务影响范围等维度的Prompt模板；将融合后的漏洞描述、PoC信息等文本输入DeepSeek-V2模型，引导其进行上下文关联和深度语义理解，并根据预设的评分标准（1~10分）输出各维度的AI辅助评分。这个动态生成的分数能够捕捉CVSS静态指标无法体现的深层次风险。

以一个真实的权限提升漏洞（CVE-2025-33073）为例，其CVSS评分为8.8（High），由于攻击需要特定配置，攻击复杂度（AC）被评为高，从而限制了总分。然而DeepSeek-V2在分析了技术细节和公开的PoC代码后，判断出特定配置在实际环境中非常普遍，且PoC代码稳定、易于使用。因此，模型给出的“利用复杂性”评分为2，“业务影响范围”评分为10，结果表明综合AI评分为9.5（Critical）。

因此，AI辅助评分成功修正了CVSS因规则僵化而导致的风险低估问题，实现了更贴近真实攻击场景的动态评估。

3.2.3 整体系统性能评估与对比分析

笔者在一个包含1 000个已标注漏洞的测试集上，对本文系统及3个基线模型进行了评估。测试集中，超高危漏洞与非超高危漏洞比例为1:4。实验结果采用五折交叉验证，取平均值，见表2。

从基线模型1到基线模型2，各项指标有轻微提升，证明了数据融合本身就能提供更准确的判断依据。从基线模型2到基线模型3，性能有较大提升，说明基于文本内容的机器学习模型远优

于静态评分规则。从基线模型3到本文系统，F1分数从0.885跃升至0.966，展现了以DeepSeek-V2为代表的大语言模型相较于传统ML在复杂语义理解、攻击逻辑和上下文关联方面的较大优势。

表2 不同模型在超高危漏洞识别任务上的性能对比					
模型	精确率	召回率	F1分数	误报率	漏报率
基线模型1	85.1%	72.5%	0.783	2.5%	27.5%
基线模型2	86.3%	74.0%	0.797	2.3%	26.0%
基线模型3	90.5%	86.5%	0.885	1.8%	13.5%
本文系统	96.2%	97.0%	0.966	0.8%	3.0%

本文系统最突出的优势在于将漏报率从传统方法的27.5%锐减至3.0%。这直接得益于AI对深层语义风险的洞察和热度模块对新兴威胁的敏锐捕捉，成功识别了大量被CVSS低估的高危漏洞，极大地降低了安全风险。相比基线模型，本文系统的精确率最高（96.2%），误报率最低（0.8%）。这表明系统在提升召回率的同时，并未牺牲准确性。多源数据的交叉验证和AI模型的精细化分析有效过滤了许多看似严重但实际利用难度极高的漏洞，为安全团队减轻了研判负担。

4 结束语

本文提出的基于多源数据融合与AI辅助多维评分的智能研判系统，相较于现有技术，在超高危漏洞的识别上展现卓越的性能。该系统通过构建信息完备的数据基础、引入AI大模型的深度语义分析能力以及结合网络热度的动态感知机制，成功地解决了传统预警系统存在的规则僵化、信息片面和预警滞后等核心痛点，显著降低了漏判风险和误报率，在F1分数上达到了较高水平，为企业关键基础设施的主动防御提供了强大而可靠的技术支撑。

参考文献：

[1] Marfo W, Tosh D K, Moore S V. Condition monitoring and

anomaly detection in cyber-physical systems[C]//Proceedings of the 2022 17th Annual System of Systems Engineering Conference. Piscataway: IEEE Press, 2022: 106-111.

[2] Jin R Y, Nan J. Combining sources from CVE and CNNVD: data analysis in information security vulnerabilities[J]. Journal of Physics: Conference Series, 2023(5): 432-440.

[3] Hassan A, Ahmad S G, Munir E U, et al. Predictive modelling and identification of key risk factors for stroke using machine learning[J]. Scientific Reports, 2024: 11498.

[4] He Y, Chen Z M, Le Goues C. PreciseBugCollector: extensible, executable and precise bug-fix collection: solution for challenge 8: automating precise data collection for code snippets with bugs, fixes, locations, and types[C]//Proceedings of the 2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE). Piscataway: IEEE Press, 2023: 1899-1910.

[5] Deepseek-Ai, Liu A X, Feng B, et al. DeepSeek-V2: a strong, economical, and efficient mixture-of-experts language model[PP]. arXiv arXiv:2405.04434.

[作者简介]

刘绪兴（1996-），男，中国移动通信集团设计院有限公司网络规划与设计优化研发武汉分中心工程师，主要研究方向为网络安全运营、数据安全、攻防渗透等。

薛姗（1986-），女，中国移动通信集团设计院有限公司网络规划与设计优化研发中心高级工程师，主要研究方向为网络安全研究、网络安全集中运营管理等。

常玲（1981-），女，中国移动通信集团设计院有限公司网络规划与设计优化研发中心高级工程师，主要研究方向为网络安全研究、网络安全集中运营管理等。

赵延毫（1992-），男，中国移动通信集团设计院有限公司网络规划与设计优化研发武汉分中心工程师，主要研究方向为软件开发，网络安全运营等。

姚傲寒（1997-），男，中国移动通信集团设计院有限公司网络规划与设计优化研发武汉分中心工程师，主要研究方向为软件开发，网络安全运营等。

周犇（1997-），男，中国移动通信集团设计院有限公司网络规划与设计优化研发武汉分中心工程师，主要研究方向为软件开发，网络安全运营等。

雷培迪（2000-），女，中国移动通信集团设计院有限公司网络规划与设计优化研发武汉分中心工程师，主要研究方向为软件开发，网络安全运营等。

张晨（1980-），男，中国移动通信集团设计院有限公司网络规划与设计优化研发中心高级工程师，主要研究方向为网络安全规划、产品研发与标准制定等。