基于AI技术和DNS数据的威胁网站分析方案

Threat Website Analysis Solution Based on AI Technology and DNS Data

威大强[1]，郑　涛[2]，由志远[1]，宋洪飞[1]，刘　果[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Qi Daqiang[1], Zheng Tao[2], You Zhiyuan[1], Song Hongfei[1], Liu Guo[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China）

摘　要：

针对网络安全领域的现状，提出一种基于分布式爬虫与混合检测引擎的恶意网站识别系统，该系统通过多层架构实现从DNS原始日志分析、域名检测、恶意域名管理的全流程管控。系统构建分布式爬虫集群，创新性地设计权重关键词规则库与AI分析相结合的检测机制，快速、高效、准确地分析恶意网站，为主动式网络安全防护提供新思路。

关键词：

DNS日志；恶意网站检测；网络爬虫；关键词匹配；AI；图片识别

doi：10.12045/j.issn.1007-3043.2025.09.009

文章编号：1007-3043（2025）09-0047-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Aiming at the current situation of network security area, a malicious website identification system utilizing distributed crawlers and a hybrid detection engine is proposed. The system achieves full process control spanning DNS raw log analysis, domain name detection, and malicious domain management through a multi-layer architecture. The system employs a distributed crawler cluster and innovatively designs a detection mechanism combining a weighted keyword rule library with AI analysis, which enables rapid, efficient, and accurate analysis of malicious websites, providing a new approach for proactive network security protection.

Keywords：

DNS log; Malicious website detection; Web crawler; Keyword matching; AI; Image recognition

引用格式：威大强，郑涛，由志远，等. 基于AI技术和DNS数据的威胁网站分析方案[J]. 邮电设计技术，2025（9）：47-51.

0 前言

随着互联网技术的迅猛发展和数字化转型的加速推进，网络安全已成为现代信息社会中不可或缺的重要组成部分，网络安全不仅关系到数据的安全性和隐私保护，还直接影响到业务的连续性和企业的声誉。这些恶意网站存活时间极短，通常仅持续数小时甚至几分钟，传统的被动防御机制难以应对。

传统的网络安全防御方案大多依赖黑名单机制和特征库匹配，即通过已知的威胁情报来识别并阻止潜在的攻击行为。尽管这种方法在一定程度上能够有效抵御已知威胁，但面对新型或变种的恶意网站时，其局限性尤为突出。首先，黑名单更新速度滞后于实际威胁的变化，导致新出现的恶意网站无法被及时识别和拦截。其次，基于特征匹配的方式对未知威胁的检测能力有限，容易被规避。此外，被动防护方案缺乏预见性和主动性，难以在威胁发生之前进行有效的防范和预警。因此，现有方案在应对快速变化的恶意网站威胁时显得力不从心，亟需一种更加智能、高效的解决方案。

针对上述问题，结合运营商自身具备的强大数据采集能力，特别是DNS日志数据的丰富资源，本文提

收稿日期：2025-07-30

出了一种创新性的主动防御方案。该方案充分利用了DNS解析过程中产生的海量日志数据，并借助先进的AI技术对其进行深度挖掘与分析，从而实现对恶意网站的实时监测与快速识别。这种基于DNS日志与AI技术相结合的方法具有多重优势：一是能够显著提高恶意网站的识别精度与时效性，二是减少了对传统黑名单和特征库的依赖，三是增强了对未知威胁的预测和防范能力。综上所述，这一创新方案不仅弥补了现有防御机制的不足，还为构建更加健壮、智能的网络安全防护体系提供了新的思路和技术手段。

1 整体方案

本方案旨在构建一套基于DNS日志分析的恶意域名识别检测系统，系统通过分析DNS日志信息，提取待检测的域名数据，并利用爬虫技术对相关域名对应的网页内容进行抓取，并对原始页面数据进行清洗、去噪和标准化处理，从中提取出可用于分析的关键特征信息，如文本内容、页面结构、链接关系等。然后，基于预先训练的人工智能模型，对输入数据进行自动化分析与判断，识别域名是否具有恶意行为，实现高效、准确的威胁检测。最终，系统将检测结果进行持久化存储，形成恶意域名库，支持后续的查询、管理与对外赋能，为网络安全防护提供实时、动态的威胁情报支撑。方案的整体架构如图1所示。

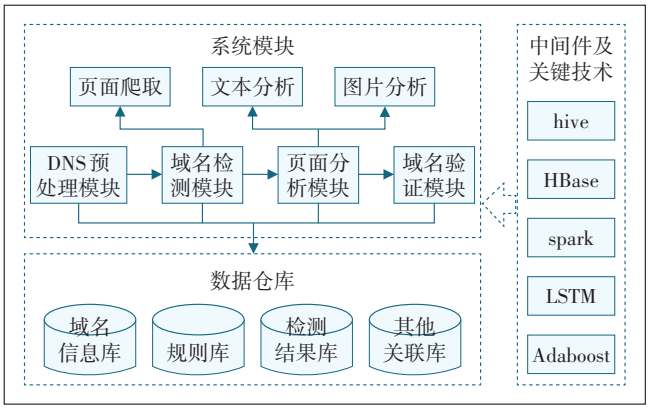

图1　整体架构

方案的设计思路如图2所示。

a）DNS日志分析。基于每日采集的DNS日志，对原始日志信息进行解析与处理，提取出相关的域名信息。同时，将提取结果与历史域名数据库进行比对，识别出当日新增的域名，为后续分析提供基础数据支持。

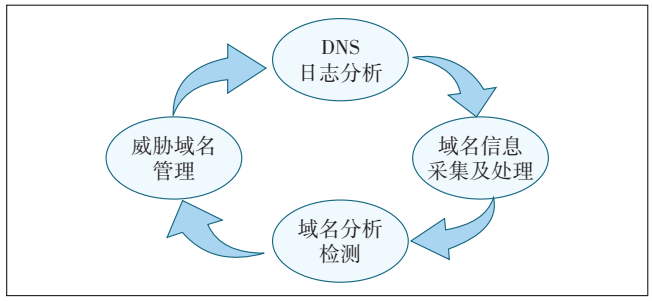

图2　方案的设计思路

b）域名信息采集及处理。针对每日识别出的新增域名，将新增域名与白名单库匹配，过滤获取未知域名信息，利用爬虫技术自动抓取其对应的网页内容，并对获取的页面数据进行清洗、去噪和标准化处理，从中提取关键特征信息，如文本内容、链接结构、页面行为等，为恶意行为分析提供高质量输入。

c）域名分析检测。通过多种检测模型相结合的方式，对页面信息以及域名信息进行分析，判断其是否为威胁网站，同时综合分析不同方式的检测模型的检测结果，并对威胁网站类型进行分类、添加置信度等级等信息，以支撑不同场景下的应用需求。

d）威胁域名管理。将最终判定为恶意的域名纳入恶意域名库，实现对外赋能与共享。同时，支持通过恶意域名反查关联的IP地址，并进一步挖掘同一IP下是否存在其他恶意域名或潜在威胁，提升整体威胁感知与溯源能力。

2 详细设计

2.1 DNS日志分析

2.1.1 目标

根据DNS日志信息获取后续需要的域名信息，提取出的相关域名信息是后续分析和检测的基础。为了确保这些宝贵的数据能够在长期使用中保持完整性和可用性，必须对其进行持久化存储，而且需要选择合适的存储引擎，选择的引擎应既能够持久化存储信息，也能够支持高效的查询。

为了节省后续的资源，减少域名的计算分析，将每日获取的全量域名信息与历史持久化数据进行比对，获取日新增域名，同时需要根据白名单过滤域名，过滤后的域名信息可以用于后续分析。

2.1.2 设计方法

DNS日志分析的主要流程如图3所示。

a）DNS日志解析与聚合模块设计[1]。该模块负责

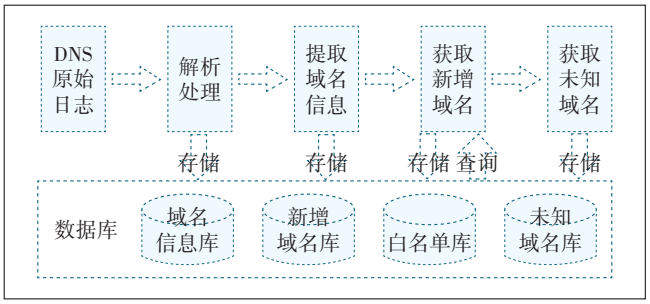

图3　DNS日志分析

对采集到的DNS日志信息进行解析处理。针对海量日志，模块设计基于分布式计算框架，启用Spark任务处理数据。核心聚合逻辑为：以“域名”作为分组键，对每日到达的所有日志记录进行分组。对于每个分组内的记录，根据分析需求，可选择执行不同的聚合操作，最终生成每个域名每日一条的聚合记录。

b）域名信息持久化存储设计[2]。鉴于传统关系型数据库难以支撑PB级数据规模和高并发点查，设计采用分布式列式数据库HBase作为持久化存储方案。其主要考量是HBase的水平扩展性能够应对海量数据增长，而其基于RowKey的快速随机读写能力能够高效支撑按域名的精确查询需求。

c）新增域名检测与处理流程设计[3]。采用分布式计算框架，结合多种大数据存储数据库，启用Spark任务，将hive中存储的每日获取的数据与历史数据进行比对，获取每日的新增域名；将新增的域名进一步进行域名白名单过滤，获取到的未知域名信息用于后续判断，识别是否为恶意域名。

2.2 域名信息采集及处理

2.2.1 目标

在域名信息采集及处理阶段，需要对每日获取的域名信息进行进一步处理。一是通过爬虫等技术获取页面信息，但由于每日需要处理的域名依旧很多，仍需要支持采用分布式的架构以及动态的扩容；二是需要对获取的页面进行标准化处理，提取关键信息，便于后续的处理。

2.2.2 设计方法

域名信息采集及处理流程如图4所示。

a）调度中心设计[4]。调度中心是整个系统中用于维护和管理爬虫集群运行状态的核心组件，由其统一管理和调度待处理的域名任务。调度中心主要分为任务分发模块和规则管理模块。

（a）任务分发模块。基于哈希一致性算法实现待处理域名任务的分片分发，将解析后的域名元数据封装为Task对象，并将Task推送到爬虫集群节点的任务缓冲队列。任务分发模块具备对爬虫集群任务状态的实时监控能力，能够根据各节点当前待处理任务的数量，实现任务的动态均衡分配，提升整体处理效率。

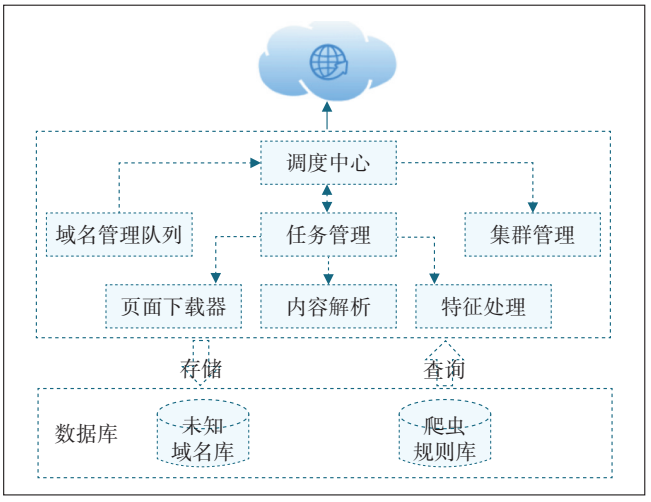

图4　域名信息采集及预处理

（b）规则管理模块。依据规则管理模块配置的策略和规则，对爬虫集群的运行进行统一管理和调度，确保任务执行的规范性与灵活性。

b）集群管理模块设计。该模块主要负责对爬虫节点的配置信息进行统一管理，主要分为2部分。

（a）集群节点管理。支持对节点进行添加、删除、修改等操作，支持根据业务需求和资源情况实现爬虫集群的动态扩缩容，从而提升系统的灵活性与资源利用率。

（b）资源调度机制管理。字段集群管理模块还具备针对单台物理机或虚拟机进行精细化资源调度的能力，基于性能等级动态调整任务配额，高性能节点任务并发数可设为基准值的1~2倍，低性能节点下调至0.5~1倍，确保整体爬虫效率处于最优状态。

c）爬虫任务模块设计[5]。爬虫任务从统一的任务队列中获取URL任务，并发高效地下载对应的网页内容。爬虫任务模块主要由以下几个核心模块组成。

（a）页面下载器。基于开源框架WebMagic实现，负责向目标域名发起HTTP、HTTPS请求并下载页面内容。该模块支持对多种异常状态码的识别与处理，如4XX、5XX等，确保在面对异常响应时具备良好的容错能力。

（b）内容解析引擎。采用Jsoup作为HTML解析

核心，配置XPath规则集提取页面中的超链接和文本内容，支持通过正则表达式过滤无效链接。对于提取出的链接，系统将根据策略决定是否进一步爬取其对应的网页内容，从而实现深度遍历抓取。

（c）特征提取与预处理模块。该模块负责对原始网页内容进行清洗与标准化处理，包括去除HTML标签、HTML转义字符等，通过中文分词和停用词过滤，提取可用于后续分析的关键特征，例如页面中的特定标签内容、关键词分布、结构化信息等，为恶意行为识别提供高质量的数据输入。

2.3 域名分析检测

2.3.1 目标

首先，通过对威胁网站的文本信息进行分析，可识别出网页中蕴含的与色情、赌博等违法内容相关的主题特征。针对网页中的文本内容，从词汇层面对页面信息进行解析和判断，用于区分色情、赌博类域名与非恶意域名。其次，对网页中的图像内容进行深度分析，进一步判断其是否为色情类图片，从而全面覆盖多维度的威胁表现形式。最后，构建综合评估模型，融合文本分析与图像识别的结果，根据不同维度的判断结果动态调整置信度评分。通过对文本信息判断结果与图片样本分析结果的加权汇总，形成对目标域名的最终综合判定，提升恶意域名识别的准确率与可靠性。

2.3.2 设计方法

域名分析检测流程如图5所示。

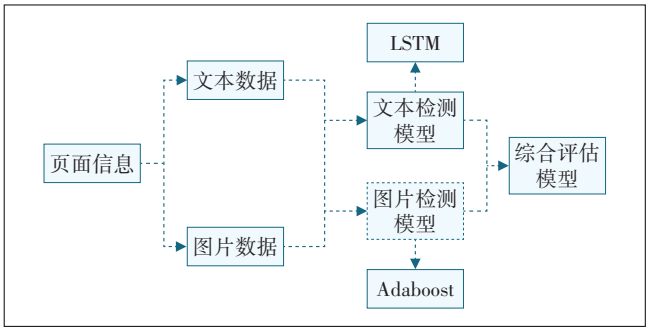

图5　域名分析检测流程

a）文本检测模型设计。

（a）威胁网站文本研究[6]。通过对威胁网站的网页文本内容的分析，针对色情、赌博、非色情赌博等3类典型的网站域名，本方案系统性地采集其网页文本数据，通过对文本进行精细化的分词处理，统计高频词汇并排序，深入挖掘不同类别威胁网站的语言模式与关键词特征。基于词频分析结果，构建了面向威胁域名检测的专业化语料库。

（b）创建基于LSTM的威胁域名文本检测模型[7-8]。该检测模型由TensorFlow框架实现，算法模型的输入是域名的网页内容编码，模型的中间处理层包括词嵌入处理、LSTM特征提取、Relu激活函数层、Dropout遗忘层和批处理标准化层等，模型的输出层是SoftMax层，将域名分成色情、赌博、非色情赌博域名3类，用于训练、检测色情和赌博域名的模型数据存储在ClickHouse数据库中，该数据库包含约50万个色情域名、40万个赌博域名以及50万个非色情非赌博域名。数据按70%的训练集和30%的测试集进行划分，并确保每个类别在训练集和测试集中的分布相对均匀，最终训练结果为模型预测的准确率高达99.74%[7]。

b）图片检测模型设计。不良图片的一个关键视觉特征是包含人脸[9]，精确检测并定位人脸对于最终判断至关重要，首先采用高效的Adaboost算法进行人脸检测[10]，获取人脸的高与宽信息h和w，人体高度一般为$7.5h$、宽度为$1.5w$，通过人脸识别算法可预估出人体区域。随后，对图像进行肤色检测，并将检测到的肤色区域与定位出的人体区域进行比对分析[11]。通过计算人体区域内肤色像素的占比，并结合人体区域的形状特征分析，实现对图片不良内容的精准识别。实验共对500张图片进行了判断，其中正常图片有300张，不良图片有200张，不良图片的判断正确率为89.5%[12]。

c）融合图片文本提取与内容分析的多模态检测[13]。大量威胁网站会将其核心信息嵌入图片中以规避纯文本检测，同时由于图片检测模型较消耗性能，故将其设计集成cnocr组件，对网页中所有图片进行OCR处理。若成功提取到有效文本，则将其输入至步骤a）中的文本检测模型进行分析。若图片中未检测到有效文本信息，则将该图片输入步骤b）进行不良图片检测。通过此方法可保证域名检测的全面、准确，同时也可保证域名检测的效率。

d）置信度量化模型设计。该模型负责综合考虑文本检测模型和图片检测模型输出的结果及其各自的置信度分数。文本模型输出类别置信度为p_text（0~1）、图片模型输出置信度为p_image（0~1），采用加权求和计算初始得分：$score = w\_text \times p\_text + w\_image \times p\_image$，其中权重$w$根据模态准确率动态调整。系统将低置信度样本（0.5<score<0.7）自动推送到审核

平台，审核结果作为标签加入训练集，每周重新训练模型参数。

2.4 威胁域名管理

2.4.1 目标

在威胁域名管理阶段，首先需对识别出的恶意域名进行集中存储，构建恶意域名库，实现数据沉淀与对外赋能。同时，还需对恶意域名进行深入分析，通过查询其对应的IP地址信息，进一步反向解析该IP下关联的其他域名，挖掘潜在的同源恶意域名。将发现的同源域名重新进行分析与处理，从而形成闭环分析流程，提升整体威胁发现与响应能力。

2.4.2 设计方法

威胁域名管理流程如图6所示。

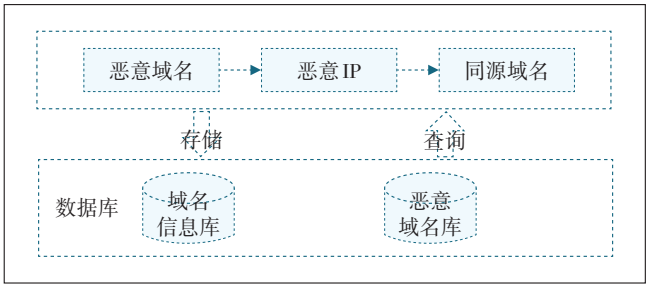

图6　威胁域名管理流程

a）情报服务设计。将分析识别出的恶意域名进行持久化存储，形成结构化的威胁情报数据库。原始数据存储于hive、ES数据库中，关联存储使用Neo4j图数据库构建域名-IP的关联图谱[14]，节点属性包含实体类型、属性值、更新时间，边属性记录关联强度，支持Cypher语句实现多跳关系查询。

b）同源域名分析设计。将已确认的恶意域名与Hbase库域名-IP信息进行匹配，获取其对应的IP地址信息[15]；随后以该IP地址为线索，再次在Hbase库IP-域名信息中进行反向匹配，查找与该IP关联的其他域名。通过这种方式可发现与恶意域名共用同一IP的潜在恶意域名，进一步拓展威胁发现范围。新获取的关联域名将作为新的输入源，重新注入到数据采集阶段，实现对恶意行为的持续追踪与深度挖掘。

3 总结

本文提出了一种基于DNS日志与人工智能技术相结合的创新性主动防御方案，有效弥补了传统被动防御机制在应对恶意网站方面的不足。该方案通过采集和分析海量DNS日志数据，结合AI模型进行特征提取与行为分析，实现了对恶意域名的高效识别与实时监测。

相较于传统方法，该方案不仅提升了检测的准确性与时效性，还具备更强的泛化能力，能够有效识别未知威胁，降低安全防护对黑名单和静态规则的依赖。同时，该方法具有良好的可扩展性和实用性，为构建智能化、自适应的网络安全防护体系提供了有力支撑，具有广泛的应用前景和推广价值。

参考文献：

[1] 田世奇. DNS流量采集系统的实现与流量分析[D]. 北京：北京邮电大学，2017.
[2] 谢地，王同喜. 基于HBase的海量数据存储和快速检索[J]. 电脑知识与技术：学术版，2019，15(4)：14-15，18.
[3] 陈晓军，姚浩浩，王月领，等. 基于DNS日志的恶意域名态势预警研究[J]. 信息技术与信息化，2021(7)：99-101.
[4] 方宇浩，倪胜巧. 网页监控分布式爬虫[J]. 现代计算机(普及版)，2015(4)：62-64.
[5] 刘小云. 网络爬虫技术在云平台上的研究与实现[D]. 四川：电子科技大学，2016.
[6] 朱国杰. 基于文本特征的不良网页检测系统的研究与实现[D]. 杭州：浙江大学，2019.
[7] 米热依·布克西. 基于DNS日志的不良域名在线检测系统设计与实现[D]. 哈尔滨：哈尔滨工业大学，2022.
[8] 李少卿. 不良文本及其变体信息的检测过滤技术研究[D]. 上海：复旦大学，2014.
[9] 唐建雄. 基于计算机视觉的人脸检测[J]. 微计算机信息，2006，22(14)：301-302.
[10] 王一丁. 实际网络环境中不良图片的过滤方法[J]. 通信学报，2009，30(S1)：103-106，113.
[11] 刘益和，刘嘉勇，袁新峰. 基于内容分析的特定图像过滤技术研究[J]. 计算机工程与应用，2006，42(24)：56-58，156.
[12] 胡柳，周立前. 基于YCbCr颜色空间的不良图片检测研究[J]. 科学技术与工程，2013，13(15)：4433-4436.
[13] 傅泉生. 融合图像语义与文本信息的色情图像判定算法研究[D]. 黑龙江：哈尔滨工业大学，2013.
[14] 唐思宇，李赛飞，张丽杰. 基于Neo4j的网络安全知识图谱构建分析[J]. 信息安全与通信保密，2022(8)：60-70.
[15] 陈俊仁. 基于域名和IP协同分析的不良站点发现系统设计与实现[D]. 黑龙江：哈尔滨工业大学，2023.

作者简介：
威大强，毕业于中国药科大学，学士，主要从事安全技术的研究工作；郑涛，高级工程师，硕士，主要从事网络安全管理及技术研究工作；由志远，毕业于西安电子科技大学，高级工程师，硕士，主要从事网络软件研发工作；宋洪飞，毕业于太原理工大学，硕士，主要从事安全技术的研究工作；刘果，毕业于武汉理工大学，学士，主要从事安全技术的研究工作。