基于 AI 人工智能技术的病毒防护体系研究与应用

聂良刚
广西财经学院大数据与人工智能学院，广西 南宁 530003

摘要：随着恶意软件的快速演变与网络攻击的智能化升级，传统防护手段难以应对不断增长的网络安全威胁。人工智能（AI）技术凭借其智能识别、自动学习和快速响应的能力，成为现代病毒防护体系的核心驱动力。为此，本文聚焦 AI 赋能的病毒防护架构设计与实际应用，探讨如何构建高效、智能的病毒防护体系，这对于今后有效应对复杂多变的网络安全环境具有重要意义。

关键词：AI 技术；病毒防护体系；智能检测；动态防御

Research and Application of Virus Protection System Based on AI Technology

Nie,Lianggang

Faculty of DB and AI, Guangxi University of Finance and Economics, Nanning, Guangxi, 530003, China

Abstract: With the rapid evolution of malicious software and the intelligent upgrade of network attacks, traditional protection methods are difficult to cope with the growing network security threats. Artificial intelligence (AI) technology has become the core driving force of modern virus protection system with its ability of intelligent identification, automatic learning and quick response. Therefore, this paper focuses on the design and practical application of AI-enabled virus protection architecture, and discusses how to build an efficient and intelligent virus protection system, which is of great significance for effectively coping with the complex and changeable network security environment in the future.

Keywords: AI technology; Virus protection system; Intelligent detection; Dynamic defense

DOI: 10.62639/sspis15.20240104

随着通信技术和电子科技的创新发展，人工智能的热度不断攀升，人工智能时代的发展趋势逐渐向网络化、信息化方向转变，使得信息资源的共享性特性愈发明显，计算机信息的安全性与防护措施的有效性也成了各领域关注的重点 [1]。根据卡巴斯基实验室的统计，2022 年全球检测到的恶意文件数量每天高达 40 万次，同比增加 5%。与此同时，网络攻击的形式逐渐智能化、自动化，诸如勒索软件、恶意广告软件和鱼叉式网络钓鱼等精准攻击手段更加猖獗，已经给众多行业的关键基础设施和数据安全带来了前所未有的威胁。《2023 年全球威胁报告》指出，约 70% 的企业曾遭遇过恶意软件攻击，且由于传统防护手段大多依赖静态特征库和行为匹配，这类手段在识别未知威胁时常常存在响应滞后或检测盲区。面对这一背景，人工智能（AI）技术因其在大数据分析、自动化学习和实时监测方面的优势，成为了现代病毒防护体系的核心驱动因素。AI 技术不仅支持复杂网络流量的实时分析，还能够从海量数据中挖掘出隐藏的异常模式，快速响应病毒的变异特征 [2]。目前，包括深信服在内的多家网络安全公司已将多智能体算法、深度学习模型和分布式架构结合应用于其防护体系中，这类 AI 驱动的解决方案能够动态优化检测模型，显著降低误报率并提升检测精度，从而为用户提供更强大的全方位病毒防护。这一创新转变标志着网络安全领域进入了一个以智能防护为基础的新时代，面对复杂多变的网络环境，AI 技术已成为提升病毒防护体系效能的关键所在。

一、基于 AI 的病毒防护体系架构设计

基于 AI 的智能防护引擎是病毒防护体系的核心组件，承担从检测、分析到响应的全流程任务，设计上充分整合多智能体算法和深度学习模型，可满足病毒快速变种和高级持续性威胁的防护需求。整个引擎的架构由多智能体算法层、模型优化层和实时响应模块构成，并在这三者之间实现高效的信息交互与反馈。

（一）多智能体算法层的创新设计

智能防护引擎的多智能体算法层由若干具有不同职责的智能体组成，每个智能体负责特定的检测或分析任务 [3]。该设计采用分布式智能体架构，能够并行化地监测网络流量、用户行为、文件属性等多维数据来源。这种分工不仅避免了传统单一模型可能面临的负载瓶颈，还增强了在面对复杂网络环境时的适应性。智能体之间采用一种类似竞赛的协同策略，若一个智能体检测到特定行为的异常特征，它会触发其他相关智能体启动高优先级分析和实时响应机制，借此在数毫秒内对潜在威胁作出反应。各智能

（稿件编号：IS-24-4-1016）

作者简介：聂良刚（1971-03），男，汉族，籍贯：广西藤县，硕士，教授，研究方向：网络，信息化，软件及算法。

基金项目：中国高校产学研创新基金 - 新一代信息技术创新项目：“基于云、本地和 AI 人工智能技术的病毒防护体系研究与应用”（基金号：2021ITA11014）。

体还配备自适应调整功能，能根据每次检测到的特征权重对自身参数进行微调，以快速适应新型攻击的变化和多样化特征。

（二）深度学习模型的层次化优化

智能防护引擎的核心模型优化层主要基于深度神经网络（DNN）和卷积神经网络（CNN），进一步辅以少量长短期记忆网络（LSTM）用于时间序列的异常分析。这些模型通过多层次架构实现，首先由浅层 CNN 提取低维特征，如文件大小、协议类型、端口号等基础属性，然后依托 DNN 层的多层感知器模型进行高维特征的复杂提取和分析，最终由 LSTM 捕获时间维度上的动态特征，形成对持续性攻击行为的更全面认知 [4]。各模型训练采用一种“少样本学习”机制，即通过少量标注样本不断调整网络参数，使系统即便在面临新的变种或未知样本时也能保持较高检测精度。此外，防护引擎对每种模型的训练过程设置了不同的迭代频率和学习率，保证了多模型体系中的每个模型都能在自己擅长的领域达到最优性能。

（三）实时响应模块的动态调整机制

在智能防护引擎的架构中，实时响应模块是病毒防护的最后一道屏障，负责将检测到的威胁实时响应和隔离处理。为实现最优响应速度，模块内部采用了一种事件优先级分级机制，将威胁事件根据危害程度和传播速度划分为不同优先级，优先级高的事件会触发更快速的响应路径，直接隔离，或拦截恶意流量。为进一步提升模型的准确性，实时响应模块还与模型优化层保持双向信息流。每次隔离或处理完成后，模块会将最新的检测信息反馈至深度学习模型，用于更新模型参数。这种双向反馈机制保证了系统在实际应用中的不断优化与学习，提升了对变异病毒的检测和防护效果。

二、AI 病毒防护体系的实际应用

（一）智能防护引擎

深信服的 SAVE 引擎在设计上深度整合了多智能体算法与分布式训练平台，实现了显著的误报率降低与检测精度提升。该技术的核心是以多智能体架构为基础，将不同的 AI 模型模块细致分工，各司其职地负责恶意样本的收集、识别、筛选与分类 [5]。具体而言，SAVE 引擎首先在系统中设置了多个并行的智能体，每一个智能体都专注于检测不同类型的威胁，如勒索病毒的变种或未知样本。这些智能体被设计为高效并行工作，能够实时扫描海量数据包，通过协同过滤技术、分类器优化和深度神经网络相结合的算法，检测出数据中的异常特征。系统使用的深度学习算法层次多样，包括卷积神经网络（CNN）和递归神经网络（RNN），使得引擎能够从行为模式上捕捉病毒特征，将恶意文件与良性数据精准区分开来。

分布式训练平台的引入有效提高了引擎的训练速度和模型响应能力，这一平台不仅支持跨服务器节点的高并发处理，还采用了分布式数据存储和计算架构，使得每个节点均具备快速处理数百万条日志的能力。分布式架构的设计让每一个服务器节点在本地生成模型，并逐步积累识别特征，从而形成一种“先端到端、再聚合”的智能防护模式。在误报处理上，SAVE 引擎设有自适应纠错机制，实时更新误判数据，借助对抗学习技术进一步优化模型，使得误报率大幅降低。引擎设计中特别设置了多层级的误报筛选器，分为初级检测、深度分析和最终确认，每一层检测过程都使用不同参数和阈值。初级检测层的误报率阈值较低，通过宽泛筛选尽量捕获潜在威胁；深度分析层则缩小了阈值范围，以更为严谨的标准对误报样本进行重检；最终确认层进一步以迭代算法对样本行为模式进行对比分析，使得误报率控制在 0.01% 以下。

具体到勒索软件防护方面，SAVE 引擎特别构建了一个快速响应的勒索行为检测模块，专门用于识别潜在的加密行为与数据劫持，该模块使用动态行为检测算法，通过识别文件加密操作的速度、目录路径变化和系统资源占用情况，对比正常数据流动特征，从而提前预警潜在的勒索行为 [6]。为了避免常规系统更新或文件操作的误判，系统设置了特定的检测参数，限定了文件读写速率的异常波动值以及进程资源消耗上限。若检测到疑似勒索操作，系统会立即隔离感染源并发出警报，同时生成事件报告供安全人员分析。在实际应用中，SAVE 引擎能够将检测频率提升至每秒百万次数据对比，达到对威胁的实时响应与防护，形成企业级用户网络的多层防护屏障。

（二）跨平台分布式防护方案

某大型企业在网络中部署了 AI 驱动的跨平台分布式防护体系，该体系以云端与边缘设备的深度协同作为防护策略的核心，显著增强了整体病毒防护能力。在实施中，云端作为全局控制中心，承担数据分析、模型训练和策略分发等重任，同时经高速数据通道不断从各边缘节点接收实时日志、流量信息以及安全事件反馈。云端使用的大规模并行计算框架允许在数分钟内处理数千万条数据包，每个数据包在入云时都经过初步的特征提取和标签标注，这些预处理步骤使用卷积神经网络（CNN）模型来快速识别潜在的异常特征，而特征提取的维度设置在 1024 项以提高覆盖率。与此同时，边缘设备作为第一道防线，负责本地的入侵检测、行为分析和威胁阻断，并在本地缓存短期内的检测模型。每个边缘设备都具备自适应学习模块，采用递归神经网络（RNN）捕捉短期内的趋势变化，例如快速识别短周期内的重复访问请求及异常带宽消耗，从而在毫秒级反应速度下自动判别并隔离可疑流量。

在数据同步过程中，边缘设备向云端定期上传汇总的检测结果和样本数据，在云端汇总

生成新模型，同时基于最新的威胁态势动态调整边缘防护策略。云端每隔数小时即刷新一次全局检测模型，并下发至所有边缘节点，更新过程自动完成，以极小的延时实现在网络内部的同步。云端部署的多层次 AI 模型，包括异常检测、深度威胁分析以及多维关联模型，可分析多源数据和跨平台攻击模式，通过一种内置的事件关联机制，将不同节点的检测结果进行整合和交叉验证。该机制能够解析各个节点的 IP、MAC 地址以及操作行为等信息，设定精确匹配参数，利用机器学习算法计算风险权重，从而判断各个节点上威胁事件之间的关联性。若云端判定某一威胁具有高传播风险，即刻向边缘设备发送控制指令，指示相关节点执行隔离操作。此外，云端还集成有实时数据流过滤模块，在边缘未能完全隔离的情况下，直接对进出的流量进行再处理，通过精细的白名单和黑名单规则降低误判风险。

针对不同操作平台的兼容需求，该分布式防护体系适配了 Windows、Linux 和 Android 等多个操作系统，通过跨平台编译器以支持多种架构的边缘设备操作。边缘设备的硬件性能差异较大，因此该防护体系提供了一种资源自适应调度算法，可动态调整边缘设备的检测频率、数据缓存时长等参数，适配设备的计算能力和网络带宽。在实际应用中，当大规模数据流如 DDoS 攻击发生时，边缘设备会自动启动流量削减机制，智能分发至负载较低的节点，并利用 AI 算法进行基于阈值的深层次流量分析。经过以上多层次、跨平台的分布式防护配置，该企业的病毒防护体系不仅能够对大规模恶意流量和复杂的跨平台威胁实现快速、准确的阻断，还能在攻击过程中动态调整防护策略，确保整个网络的安全与稳定。

（三）云端环境中的病毒防护

在云端环境中，为应对高并发请求的需求，AI 驱动的病毒防护体系采用了智能调度和资源优化技术，实现了实时网络流量分析以及病毒样本的识别。整个防护体系首先基于分布式计算架构，将云端资源分割成多个虚拟化计算单元，这些单元在实际运行中通过容器技术隔离，各单元内置深度学习模型和智能调度算法。网络流量的分析任务被分配到这些虚拟单元，避免资源冲突，调度逻辑依据流量的峰谷动态调整计算资源，利用负载均衡机制将大流量分发到空闲单元，达到快速处理的目的。云端 AI 模型部署上采用多层卷积神经网络（CNN）与长短期记忆网络（LSTM）结合的架构，以便在高并发环境中检测恶意流量和异常行为，识别潜在的病毒样本。

该防护体系运行的每一轮数据分析过程中，首先由预处理模块筛选出异常的访问行为或潜在威胁。预处理模块会提取访问频率、IP 地址、传输协议、数据包大小等特征，并以此为输入参数进入 CNN 模型，CNN 模型的特征提取层以卷积核大小为 3x3，深度为 256 层，能够准确捕获流量中的细微特征，精度误差控制在 0.5% 以内。对于长时间出现的异常流量，系统则引入 LSTM 模型进行时间序列分析，确保检测到持续性威胁。若模型判定流量中包含疑似病毒样本，则会将该样本隔离并标记，进一步进入深度分析阶段。深度分析阶段使用了一种特征图优化算法，将样本特征与已有的病毒数据库进行交叉对比，同时引入自然语言处理（NLP）模型对样本代码特征进行语义分析，识别病毒的家族和变种，做到极高的识别准确率。

为了应对云端环境中的资源消耗问题，该防护体系还配备了资源调度优化模块，模块基于 AI 实时计算出最佳的资源配置方案，根据流量压力调整 CPU、内存和带宽的占用比例。例如，当流量峰值达到 80% 负载时，系统自动分配额外的 CPU 和内存，优先调度给异常流量分析单元。为了保证防护过程的持续性和稳定性，系统对分析模型每 4 小时执行一次热更新，利用云端分布式训练平台进行样本学习，更新后的模型立即生效，及时应对最新的病毒变种。

三、结束语

综上所述，基于 AI 的病毒防护体系已展示出显著的技术优势，智能防护引擎的实时监测、动态响应和自适应调整，为高效、精准的威胁防护提供了坚实保障，分布式架构与云端协作进一步扩展了系统的处理能力和防护覆盖面。在当前和未来的网络环境中，AI 技术无疑将成为病毒防护的核心驱动因素。然而，随着威胁类型的多样化和对抗性技术的不断提升，病毒防护体系还会面临接踵而来的新挑战，我们必须在优化现有防护方案的同时，持续投入研究和创新，完善 AI 驱动的防护体系，更加灵活、高效地应对未知的威胁。

参考文献：

[1] 郭靖．基于人工智能的化工企业计算机网络安全系统应用——评《化工信息化技术概论》[J]．化学工程，2024，52（10）：98.
[2] 林云柯．人工智能会梦到鬼故事吗？——从“文学模型”到计算机病毒 [J]．中国图书评论，2024，（10）：8-19.
[3] 马遥．基于大数据及人工智能技术的计算机网络安全防御系统设计 [J]．信息与电脑（理论版），2020，32（04）：208-209.
[4] 王萍利．基于人工智能技术的化工企业计算机网络安全防御系统设计 [J]．粘接，2021，47（08）：106-109+122.
[5] 龚娇，国颌娜．基于人工智能技术的计算机网络安全防护系统的设计和实现 [J]．软件，2022，43（04）：48-50.
[6]2021 年《计算机研究与发展》专题（正刊）征文通知——人工智能安全与隐私保护技术 [J]．计算机研究与发展，2020，57（10）：2200.