 DOI: https://doi.org/10.12345/bdai.v5i9.22283

Research on the Application of Artificial Intelligence and Big Data Technology in Biomedical Computer Network Security Defense

Gaoshan Zhu[1] Mengqi Sun[2*]

1. Shanghai Fuhong Hanlin Biotechnology Co., Ltd., Shanghai, 200233, China
2. Shanghai Fosun Group, Shanghai, 200010, China

Abstract

The current era is the information age and digital age. The application and popularization of big data technology and information technology have brought more convenience to people's production and life, but also increased the risk of information leakage. Strengthening computer network security defense is essential. The reasonable application of artificial intelligence technology and big data technology in computer network security defense can better ensure the effectiveness of computer network security defense, avoid information loss, system crashes and other related problems caused by system poisoning and attacks. Therefore, combined with the actual needs of computer network security defense, it is necessary to apply artificial intelligence technology and big data technology reasonably. This paper also focuses on this and discusses how to better utilize the technical advantages and characteristics of artificial intelligence technology and big data technology in computer network security defense to enhance the effectiveness of network security defense.

Keywords

artificial intelligence; big data technology; computer network security defense; application requirements

人工智能和大数据技术在生物医药计算机网络安全防御中的应用研究

竹高山[1] 孙梦琪[2*]

1. 上海复宏汉霖生物技术股份有限公司，中国·上海 200233
2. 上海复星集团，中国·上海 200010

摘 要

现今时代是信息化时代和数字化时代，大数据技术、信息技术的应用和普及为人们的生产生活带来了更多的便捷，但同样也增加了信息泄露风险。加强计算机网络安全防御十分必要，在计算机网络安全防御中人工智能技术和大数据技术的合理应用可以更好地保障计算机网络安全防御效果，避免系统中毒被攻击等引发的信息丢失、系统崩溃等相应问题，因此结合计算机网络安全防御的实际需求，合理应用人工智能技术和大数据技术是十分必要的，论文讨论了在计算机网络安全防御中如何更好地运用人工智能技术和大数据技术的技术优势和技术特性来提升网络安全防御效果。

关键词

人工智能；大数据技术；计算机网络安全防御；应用要求

1 引言

信息技术的推广与普及为人们的信息交互和资源共享提供了更多的助力和便捷，提高了人们生产生活的效率和质量，但是这些信息技术的融入和应用在便捷人们的同时也带来了新的风险和新的问题，如何保障计算机网络安全是现今时代必须着重考量的关键重点，大数据技术和人工智能技术的应用可以较好地实现这一目标，可以从以下几个维度着手做出优化和调整。

2 构建多层级的平台防线

就现阶段来看，在计算机网络平台运行的过程中其面临的威胁是相对较多的，具体可以划分为恶意软件威胁、恶意站点威胁、恶意攻击威胁、恶意团伙威胁四大类别，如图

【作者简介】竹高山（1984–），男，中国浙江嵊县人，博士，从事网络空间治理体系中用户数据安全及隐私保护策略研究。

【通讯作者】孙梦琪（1985–），女，中国上海人，硕士，从事数字经济安全技术研究。

1 所示，在这样的背景下建立单独的一道防线往往无法保证计算机网络平台的安全性，需要通过多级平台防线的构建来更好地抵御恶意威胁，具体可以从以下几个方面展开分析。

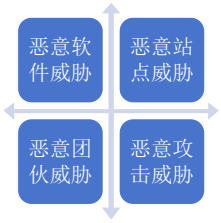

图 1 恶意威胁分类

首先，可以通过边界防护来提高各类恶意威胁的防范能力，如可以通过防火墙设置、状态检测、环境检查等多种方式来更好地抵御外界威胁，最大程度地减少病毒的侵入，进而更好地保障数据安全和信息安全。

其次，可以通过流量检测的方式在保障平台运行稳定性的基础之上提高防范能力，可以通过 XDR 态势感知完成高级威胁检测、加密流量检测、暗网流量检测和脆弱性检测等多项检测任务，提高风险感知能力 [1]。

再次，可以以响应闭环为中心对该防线作出优化和调整，如通过 MSS 安全托管服务，实现对网络平台 24 小时持续监测，及时发现在网络平台运行过程中存在的各类安全风险和安全问题，提高风险感知能力。通过安全托管服务的有效应用确保事故闭环率达 100%，威胁检测率达 99% 以上，一旦安全托管发现存在网络风险则会及时发送告警信息，同时可以通过人工智能技术的有效应用配合大数据技术对接专家系统，根据告警信息中的关键词推送相应的解决方案和处理路径，为安全风险的快速解决提供更多的帮助。

最后，为了避免前三道防线无法有效发现安全风险进而带来数据丢失、系统崩溃等相应问题，第四道防线以数据恢复为主，建立兜底机制，即在系统运转的过程中自动收录备份相应的信息数据上传至云端或上传至固定的储存器当中，如果系统遭到恶意攻击出现信息丢失、系统崩溃等相应问题，操作人员则可以通过启用备份的方式来最大化地降低信息丢失、系统崩溃所带来的影响和损失。如果恶意攻击导致系统崩溃，在系统重构上相关单位往往也需要花费大量的时间精力和资源，在这样的背景下可以在第四道防线建立完善业务系统恢复机制，通过启动恢复机制来最大化地降低各种恶意威胁所带来的影响和损失 [2]。

3 完善引擎体系

完善和优化引擎体系形成层层递进的管理闭环也可以更好地保障计算机网络平台使用的安全性，在引擎体系优化和完善的过程可以围绕以下几个要点做出优化和调整，如图 2 所示。

首先应加强数据接入治理，该层级设计的主要目的是为了完成原始日志的录入，在该环节需要确保上传的数据信息符合标准，因此相关单位在完善和优化平台安全防御机制的同时也需要确立完善的数据上传标准，要求相关工作人员在数据上传的过程中注意格式调整，为数据接入治理提供更多的助力。

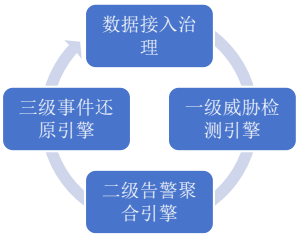

图 2 引擎系统构建要点

在此之后设计一级威胁检测引擎，主要检测项目包含终端威胁检测、网络威胁检测、行为基线检测和自定义威胁检测等等，在一级威胁检测引擎中可以设计 IOC 引擎、IOA 引擎、语义引擎、流式引擎、UEBA 自定义引擎、基线检测引擎等相应的引擎，最大化地提高威胁检测能力和检测水平，及时发现风险和问题 [3]。

然后设置二级告警聚合引擎，通过削减归并的方式拦截风险、识别问题，在二级告警聚合引擎中须满足多元日志融合需求、告警多级规定需求、无效日志过滤需求、网网关联需求、网端关联需求和告警定性需求。通过扫描器识别、人机识别行为、基线识别和攻击特征融合类型融合、误报校验、业务识别等相应方法来更好地提高告警归并能力，简而言之，通过二级报警聚合引擎的设计和优化在提高风险预知能力和响应能力的基础之上，还需要对识别到的风险信息进行定性分析，判断该风险信息是否真实，在确保风险信息真实的基础之上识别风险信息，并做好资源共享，避免出现风险误报等情况，同时也通过告警归并的有效应用在出现风险问题时第一时间做好信息公示，让相关工作人员可以及时地做出反应，快速启动应急预案，进而最大化地降低风险和损失。

最后，设计三级事件还原引擎，三级事件还原引擎设置的主要目的是为了完成攻击链还原，通过单终端攻击链还原、多终端攻击链还原、入口点溯源、影响面分析、弱信号挖掘、自定义建模分析、威胁实体关联、威胁阶段关联、因果关联、威胁图谱绘制等多种方式来更好地明确风险问题的构成原因，从构成原因出发，及时发现计算机网络平台存在的安全风险和安全漏洞，同时也通过攻击链还原来分析风险问题的解决方法和处理方案，提高问题解决的效率和质量。

4 做好层级功能优化

做好层级功能优化可以为计算机网络安全防御系统的构建奠定良好的基础和保障，在层级功能优化的过程中应当围绕如下几个要点：

首先，应当突出基础设施层的虚拟化功能，在基础设施层构建和分析的过程中除了需要购入必要的硬件设施以

外，还需要通过大数据技术尤其是大智移云技术的有效应用配合硬件资源虚拟化功能来实现对硬件资源的分配和共享，这可以更好地提高计算机网络安全系统的集成能力和并发能力。同时，为了给工作人员提供更多的便捷和辅助，可以在网络平台系统构建的过程中设计数据采集模块，为数据信息的收集整合分析和共享提供更多的助力。在数据采集及共享的过程中，可以借助人工智能技术和大数据技术来设置智能包过滤功能，在提升数据共享效率和质量的同时及时发现共享数据中是否存在安全风险 [4]。

其次，在计算机网络安全防御系统优化过程中应当突出中间件层的管理功能。一般情况下，在计算机网络安全防御系统中中间件层的主要功能是完成数据的输入和输出，科学分配系统资源，完成安全访问控制，并对系统的运行状态进行监控，进而确保系统能够正常运转稳定运行，避免系统崩溃、数据丢失等相应问题。在中间件层设计和功能优化的过程中可以通过大数据技术和人工智能技术等相应现代化技术的有效应用来完善中间件层的管理功能，使中间间层的资源分配能力、安全监测能力和负均衡负载能力都得到有效提升。借助大数据技术人工智能技术等相应技术的技术优势，在中间件层管理功能丰富和优化的过程中除了需要实时监测系统平台以外，还需要注意的是随着时代的不断发展计算机网络安全风险的构成变得日趋复杂，病毒种类和特征也在不断变化，为此需要利用人工智能学习性相对较强的优势，自动更新病毒特征码；同时，为了最大化地降低试错风险，可以利用大数据技术自动收集整合互联网上其他网络安全公司公布的病毒特征码，丰富数据库，进而更好地发现未知的病毒。此外，还可以设计防御效果评估功能，更好地检测和分析过去一段时间内计算机网络安全防御系统的防护功能效果，通过定期评估及时发现计算机网络安全防御系统存在的欠缺和不足，并找到相应的解决对策和处理方案，通过不断总结、评估、分析、优化的方式来实现系统的完善 [5]。计算机网络安全防护体系如图 3 所示。

图 3 计算机网络安全防护体系

最后，应当突出应用层的服务功能，大数据技术及计算机网络系统平台构建的最终目的是为了更好地满足人们系统应用需求，便捷人们的生产生活，因此在网络安全防护系统构建和优化的过程中也必须充分考虑到用户的使用需求和使用体验，确保计算机网络平台能够为用户提供更加便捷稳定的服务。可以通过用户注册功能、用户登录功能、访问控制功能、权限分配功能、系统交互功能、非法入侵检测功能、系统备份及恢复功能等相应功能的设置与优化来更好地提高应用层的服务能力和服务效果，强化使用者的使用体验。这其中需要尤为引起关注和重视的是对权限分配功能作出优化和调整，一般情况下，计算机网络防护系统都应用于企业单位的内部网站平台，而企业单位在各部门工作落实的过程中会因工作内容的差异、工作责任的划分导致不同工作人员工作任务存在较大区别，但有一个共同特性即在各项工作落实过程中都需要一定的数据信息作为参考，计算机网络平台虽然提高了网络数据的共享能力，但也增加了数据风险。权限分配功能的设置则是根据不同部门工作人员的工作需求和工作内容确立信息阅览权限，当工作人员登录网络平台以后，系统会根据工作人员输入的工号确定工作人员的信息阅览权限，在满足工作人员的信息阅览需求基础之上通过权限设置来避免信息泄露或丢失等风险，此外在用户登录后还会通过实时监控来监测用户的登录行为并自动记录用户查阅了哪些文件，如果出现信息泄露丢失、信息丢失等问题，可以通过数据追溯来完成责任追溯 [6]。

5 结语

大数据时代下信息技术和互联网技术的应用和普及已经成为了当今的时代特征，人们在受益于大数据技术及人工智能技术等相应现代化技术的同时也承担着较大的数据安全风险，为了更好地把握网络这把双刃剑，可以通过引擎体系优化、多层级防护及各层级功能完善的方式保障信息安全和系统安全，提高风险识别响应和处理能力。

参考文献

[1] 齐德林.基于大数据技术的计算机网络安全防御系统设计方案[J].数字通信世界,2024(6):52-54.

[2] 王丽.基于大数据技术的计算机网络安全防御应用[J].信息与电脑(理论版),2023,35(19):199-201.

[3] 邱玲.大数据技术在计算机网络信息安全处理中的实践分析[J].信息记录材料,2023,24(3):83-85.

[4] 宋午阳,张尼.基于大数据及人工智能技术的网络安全防御系统设计策略[J].网络安全技术与应用,2022(7):56-57.

[5] 苗敬峰,李强.大数据技术在计算机网络信息安全问题中的应用研究[J].中国新通信,2021,23(12):77-78.

[6] 李小康.大数据技术在计算机网络信息安全问题中的应用探析[J].无线互联科技,2021,18(7):86-87.