

基于人工智能技术的电力监控系统网络安全防护技术研究

田福宪

国家电投集团甘肃电力有限公司 甘肃 兰州 730030

摘要: 当今社会, 电力供应至关重要, 电力监控系统是保障电力稳定运行的核心。但它面临诸多网络安全威胁, 如黑客攻击、恶意软件和DDoS攻击等。人工智能技术为其网络安全防护带来曙光, 它具有学习推理、处理模糊信息以及计算成本低的显著优势。基于人工智能的防护技术涵盖入侵检测、漏洞管理等关键领域, 在智能防火墙、垃圾邮件检测等方面也有具体应用。通过强化安全区域边界访问控制等防护策略, 能够有效提升电力监控系统的网络安全性, 为电力稳定供应保驾护航。

关键词: 基于人工智能技术; 电力监控系统; 网络安全防护; 技术研究

引言: 在当今数字化时代, 电力监控系统对保障电力稳定供应至关重要。然而, 其网络安全面临着诸多严峻挑战。黑客攻击、恶意软件肆虐以及DDoS攻击频发, 严重威胁着系统的正常运行和数据安全。传统的网络安全防护技术在应对复杂多变的网络威胁时, 逐渐显现出局限性。人工智能技术凭借其独特的优势, 为电力监控系统网络安全防护带来了新的思路和方法。深入研究基于人工智能的防护技术, 对于提升电力监控系统的安全性具有重要的现实意义。

1 电力监控系统面临的网络安全威胁分析

1.1 黑客攻击

黑客攻击是电力监控系统面临的一大严重威胁。黑客通常凭借高超的技术手段, 试图突破系统防护壁垒。他们会利用系统存在的漏洞, 比如软件设计缺陷、安全配置不当等。一旦成功入侵, 黑客可能窃取关键电力数据, 像电网运行参数、用户用电信息等, 这会对电力系统的正常运营和用户隐私造成极大损害。部分黑客还可能恶意篡改数据, 干扰电力调度指令, 引发电力供应的混乱, 甚至造成局部停电事故, 严重影响社会生产生活秩序。

1.2 恶意软件

恶意软件在电力监控系统中的威胁不容小觑。随着移动互联网、物联网等技术在电力领域的广泛应用, 恶意软件入侵途径增多。例如通过移动终端、外部存储设备等进入系统。像勒索病毒, 具有隐蔽性、破坏性和传染性, 一旦潜入调度数据网络, 会加密重要数据, 向电力企业勒索赎金, 若不及时处理, 可能导致整个生产网络瘫痪。蠕虫病毒则可自我复制、传播, 占用大量系统资源, 使电力监控系统运行缓慢甚至崩溃, 严重威胁电力系统数据安全与稳定运行。

1.3 DDoS攻击

DDoS (分布式拒绝服务) 攻击旨在使电力监控系统网络服务中断。攻击者操控大量被感染的计算机组成僵尸网络, 向目标系统发送海量HTTP请求和流量。这些错误流量会充斥系统网络, 耗尽其网络带宽、服务器资源等, 导致系统无法正常响应合法用户请求。在电力监控场景下, DDoS攻击可能致使监控数据传输受阻, 工作人员无法实时掌握电网运行状态, 影响电力调度决策。而且, 攻击期间黑客还有可能借机渗入数据库, 窃取敏感信息, 对电力系统网络安全造成多方面严重破坏^[1]。

2 人工智能技术在网络安全防护中的优势

2.1 学习推理能力

人工智能具备强大的学习推理能力, 能从海量网络数据中自动挖掘特征与模式。其可收集电力监控系统内正常及异常的网络行为数据, 如通信流量、设备操作指令等。通过机器学习算法, 对这些数据进行深度分析, 构建正常行为模型。一旦监测到实际行为偏离模型, 便迅速推理判断是否存在安全威胁。比如面对新型黑客攻击手段, 传统防护技术难以识别, 但人工智能可依据已学习到的相似攻击模式特征, 推理出攻击意图, 及时预警并采取防御措施, 有效应对不断变化的网络威胁, 持续提升防护能力。

2.2 模糊信息处理能力

电力监控系统网络环境复杂, 存在大量模糊信息, 如不确定来源的网络连接、不完整的异常事件信息等。人工智能凭借模糊逻辑、神经网络等技术, 可有效处理此类模糊信息。例如, 当系统检测到一个来源不明但行为疑似恶意的网络连接时, 人工智能能综合分析其通信协议、数据包内容、连接频率等模糊信息, 通过复杂的算法评估风险等级, 判断是否为恶意连接。相比传统防

护技术对精确规则的依赖,人工智能的模糊信息处理能力,使其能在复杂模糊的网络环境中,更准确地识别潜在威胁,保障电力监控系统安全。

2.3 计算成本低

在电力监控系统网络安全防护中,人工智能技术在计算成本方面具有显著优势。传统防护技术常需投入大量硬件资源与人力进行复杂运算及分析,而人工智能利用算法和模型,可在相对较少的硬件资源上实现高效处理。以入侵检测为例,人工智能算法部署在普通服务器上,通过优化的数据处理流程,对海量网络流量数据进行实时分析,识别入侵行为,无需依赖昂贵的高性能计算设备。并且,其自动化的检测与预警机制,减少了人力监测成本,以较低的计算成本实现对电力监控系统网络安全的高效防护。

3 基于人工智能的电力监控系统网络安全防护关键技术

3.1 入侵检测与防御技术

基于人工智能的入侵检测与防御技术,通过机器学习和深度学习算法,对电力监控系统的网络流量、设备操作日志等数据进行实时分析。它能够精准识别正常行为模式,并敏锐察觉偏离该模式的异常流量与操作,进而判定是否存在入侵行为。一旦监测到某一设备通信流量在短时间内大幅增长,且通信目标异常,系统就能迅速触发预警,并自动采取阻断连接、限制访问等防御措施。相较于传统基于规则匹配的入侵检测,人工智能技术能够自适应网络环境变化,有效识别新型未知攻击,显著提升电力监控系统的安全防护能力。

3.2 漏洞管理与风险评估技术

在漏洞管理方面,人工智能技术可对电力监控系统的软件代码、配置文件等进行深度扫描。运用自然语言处理技术解析代码逻辑,结合机器学习算法识别潜在漏洞,如缓冲区溢出、SQL注入等漏洞隐患。对于发现的漏洞,利用大数据分析技术评估其风险等级,综合考量漏洞的利用难度、影响范围以及可能造成的损失等多维度因素。

3.3 数据安全保护技术

电力监控系统数据至关重要,人工智能的数据安全保护技术涵盖数据加密、访问控制与数据完整性保护等方面。在数据加密上,利用量子密钥分发结合人工智能算法生成高强度加密密钥,保障数据在传输与存储过程中的保密性。在访问控制方面,基于人工智能的身份识别技术,如人脸识别、指纹识别等,结合行为分析,动态判断用户访问权限。例如,当用户登录系统进行操作

时,系统不仅验证其身份信息,还会分析其操作行为模式是否与以往一致,若出现异常则限制访问。对于数据完整性保护,采用区块链技术结合人工智能算法,对数据进行哈希运算并存储在区块链上,实时监测数据是否被篡改,确保电力监控系统数据的安全性与可靠性。

3.4 安全态势感知与预警技术

安全态势感知技术利用人工智能对海量电力监控系统安全数据进行采集、分析与融合,包括网络流量数据、设备状态信息、安全事件日志等。通过构建复杂的态势感知模型,如基于深度学习的时空关联模型,能够从多个维度全面、实时地展现系统安全状态。例如,分析不同区域电力设备的运行状况、网络连接的稳定性以及外部网络攻击的趋势等,预测潜在安全威胁。一旦发现安全态势恶化趋势,系统立即发出预警,提醒运维人员提前采取防范措施。该技术使电力监控系统从被动防御转变为主动防御,有效应对不断变化的网络安全挑战^[2]。

4 人工智能在电力监控系统网络安全防护中的具体应用

4.1 智能防火墙

智能防火墙借助人工智能技术,能够超越传统防火墙基于静态规则的防护模式。它运用机器学习算法,实时分析电力监控系统的网络流量。通过对正常流量特征的持续学习,建立起精细的流量行为模型。一旦网络流量出现偏离模型的异常情况,如短时间内大量来自特定IP的连接请求,智能防火墙可迅速判定这可能是攻击行为,并自动调整访问控制策略,阻止异常流量进入系统。同时,它还能依据系统运行状态和安全威胁变化,动态优化防护规则,极大提升了防火墙对新型、未知攻击的抵御能力,有效保障电力监控系统网络边界安全。

4.2 垃圾邮件检测

在电力监控系统中,垃圾邮件不仅占用大量网络带宽,还可能携带恶意软件或钓鱼链接,威胁系统安全。人工智能技术用于垃圾邮件检测时,通过对海量邮件样本进行深度学习,分析邮件的发件人信息、主题、正文内容、链接特征等多维度数据。例如,基于自然语言处理技术解析邮件正文语义,判断其是否包含可疑信息。经过训练的人工智能模型能够精准识别垃圾邮件,将其拦截在系统之外,大幅减少员工误点垃圾邮件带来的安全风险,确保电力监控系统内邮件通信的安全与高效。

4.3 人工神经网络技术

人工神经网络技术在电力监控系统网络安全防护中发挥着关键作用。以入侵检测为例,构建的人工神经网络可模拟人脑神经元的工作方式,对系统中的网络流

量、设备操作等数据进行并行处理与深度分析。通过对大量正常和异常数据的学习训练,神经网络能够精准捕捉到细微的异常模式。一旦检测到异常,迅速发出警报。并且,随着系统运行和新数据的输入,人工神经网络能够不断自我优化、更新模型,持续提升对各类复杂网络攻击的检测与防御能力,为电力监控系统的稳定运行筑牢安全防线。

5 基于人工智能的电力监控系统网络安全防护策略

5.1 强化安全区域边界访问控制能力

借助人工智能构建的智能访问控制模型,可对电力监控系统不同安全区域间正常的访问行为进行持续学习。它会深入分析源IP、目的IP、访问时间、传输协议等多维度数据,形成精准的访问行为模式库。一旦监测到异常访问请求,如非授权IP在特定敏感时段试图访问关键生产区域,且访问频率远超正常范围,模型便能依据学习成果,迅速识别该行为异常,并自动触发阻断机制,将非法访问拒之门外。同时,利用深度学习算法,模型能根据系统业务的动态变化,实时更新访问控制规则,让安全区域边界始终保持高效、可靠的防护状态,有效抵御外部恶意渗透,确保系统核心区域的安全与稳定。

5.2 提高网络内、外入侵和恶意代码防御能力

基于人工智能的入侵检测与防御系统,可对电力监控系统网络流量进行7×24小时实时监测。对内,它能敏锐捕捉内部设备间的异常通信情况,若某设备突然向众多其他设备发送格式异常、协议不明的数据包,系统会立即判定可能存在内部入侵或恶意代码传播风险,并迅速采取隔离措施,防止威胁扩散。对外,运用机器学习技术分析外部网络连接请求,精准识别常见攻击模式,如DDoS攻击时流量的异常暴增、特定端口的密集扫描等特征。此外,系统还能对下载文件、邮件附件等进行恶意代码深度扫描,基于人工智能的病毒查杀技术能够识别新型、变种恶意代码,从内到外全方位为电力监控系统筑牢抵御入侵及恶意代码的坚固防线。

5.3 提高违规内联、外联检测能力

依托人工智能的行为分析技术,可建立起电力监控系统内设备与人员精确的正常内联、外联行为基线。通过持续监测设备网络连接状态,能及时发现设备是否存在私自连接外部网络的违规操作,或是内部不同安全区域设备间未经授权的互联行为。例如,通过深度分析网

络连接日志,若发现办公区设备在未获许可的情况下,尝试与生产控制区网络建立连接,人工智能系统可凭借对正常行为模式的学习记忆,快速察觉并发出告警。同时,对于员工移动设备接入公司网络的行为,系统也会进行严格监控,避免因违规内联、外联导致敏感信息泄露,或引入外部未知安全风险,维护电力监控系统网络架构的合规性与安全性。

5.4 提高系统内主机病毒防范能力

在电力监控系统内的主机上部署基于人工智能的防病毒软件,该软件借助对海量病毒样本的深度学习,可精准识别已知和未知病毒的行为特征。软件会持续监控主机的进程活动、文件读写操作等关键行为,一旦发现某进程出现频繁修改关键系统文件、异常占用大量系统资源等疑似病毒感染的行为,便会立即启动高效的查杀机制,清除病毒威胁。此外,利用人工智能技术,软件还能实时更新病毒库,确保及时应对层出不穷的新型病毒威胁。并且,定期对主机进行全面深度扫描,及时排查潜在风险,为电力监控系统内主机营造安全稳定的运行环境,有力保障系统核心设备的平稳运转^[3]。

结束语

在数字化与智能化深度融合的当下,电力监控系统的网络安全防护极为关键。人工智能技术的引入,为解决复杂网络安全问题提供了有效途径。通过强化安全区域边界访问控制、提升内外入侵及恶意代码防御能力、加强违规内联外联检测,以及提高主机病毒防范水平,电力监控系统的安全防护体系得以不断完善。但网络安全威胁持续演变,未来仍需持续深化人工智能技术在电力监控系统中的应用研究,进一步提升系统的自适应防护能力,为电力系统安全稳定运行筑牢坚实防线,助力电力行业在安全可靠的环境中实现高质量发展。

参考文献

- [1]陆雄,周子富.电力监控系统网络安全防护技术[J].网络安全技术与应用,2022(12):10-11.
- [2]吴春晖.网络安全领域中人工智能技术的应用探讨[J].网络安全技术与应用,2022(12):8-10.
- [3]范铜川,司鲲鹏.人工智能在电力监控系统网络安全防护技术的应用探究[J].信息与电脑(理论版),2023,31(23):93-94.