人工智能在广播电视网络安全中的研究与应用

李建华
宁夏广播电视台　宁夏　银川　750000

摘　要：随着广播电视行业数字化、网络化发展，其网络安全面临诸多威胁。本文围绕人工智能在广播电视网络安全中的应用展开研究，先阐述人工智能与广播电视网络安全的相关概述，接着构建包含数据采集与预处理层、威胁感知与分析层等的技术架构，进而探讨智能威胁检测、自动化安全审计等关键应用场景。研究表明，人工智能能提升广播电视网络安全防护的智能化水平，有效应对各类安全风险，为广播电视行业的稳定发展提供安全保障，对推动广播电视网络安全体系升级具有重要意义。

关键词：人工智能；广播电视；网络安全；技术架构；关键应用

引言：广播电视作为重要的信息传播载体，关乎社会舆论引导与公共文化服务，其网络安全至关重要。然而，当前广播电视网络面临恶意攻击、数据泄露等安全威胁，传统安全防护技术存在响应滞后、检测精度低等问题，难以满足复杂的安全需求。在此背景下，人工智能凭借其强大的数据处理、分析和预测能力，为广播电视网络安全防护提供了新的解决方案。本文旨在深入研究人工智能在广播电视网络安全中的应用，通过分析技术架构与关键应用场景，为提升广播电视网络安全防护能力提供思路，助力广播电视行业筑牢网络安全防线。

1 人工智能与广播电视网络安全概述

在数字化浪潮推动下，广播电视网络加速向数字化、网络化、智能化转型，既丰富了内容传播形式、提升了用户视听体验，也面临着愈发严峻的网络安全挑战。当前，黑客攻击手段持续升级，从基础网络扫描到高级持续性威胁（APT），试图窃取关键数据、干扰节目正常播出；恶意软件肆意传播，可能破坏系统功能、篡改节目内容；数据泄露事件频发，不仅侵犯用户隐私，更会损害广电机构的声誉与运营稳定性。人工智能技术的兴起为广电网络安全防护提供了新路径。其强大的数据处理与分析能力，能从海量网络数据中快速识别异常模式，精准检测潜在威胁；依托机器学习算法，可实现自我优化进化，适应动态变化的安全环境；自动化决策与响应机制，还能在安全问题出现时即时行动，最大限度降低损失。将人工智能融入广电网络安全领域，可构建主动、智能、高效的防护体系，为广电网络安全稳定运行筑牢屏障[1]。

2 人工智能在广播电视网络安全中的技术架构

2.1 技术架构概述

人工智能在广播电视网络安全中的技术架构是一个有机整体，旨在通过分层处理和协同工作，实现对广播电视网络安全的全面监测、精准分析和快速响应。该架构以数据为核心驱动力，从数据的采集与预处理开始，经过威胁感知与分析，到智能决策与响应，最后通过可视化与交互层为用户提供直观的管理界面，形成一个闭环的安全防护体系。各层之间相互关联、相互影响，共同为广播电视网络安全保驾护航。如下图1所示

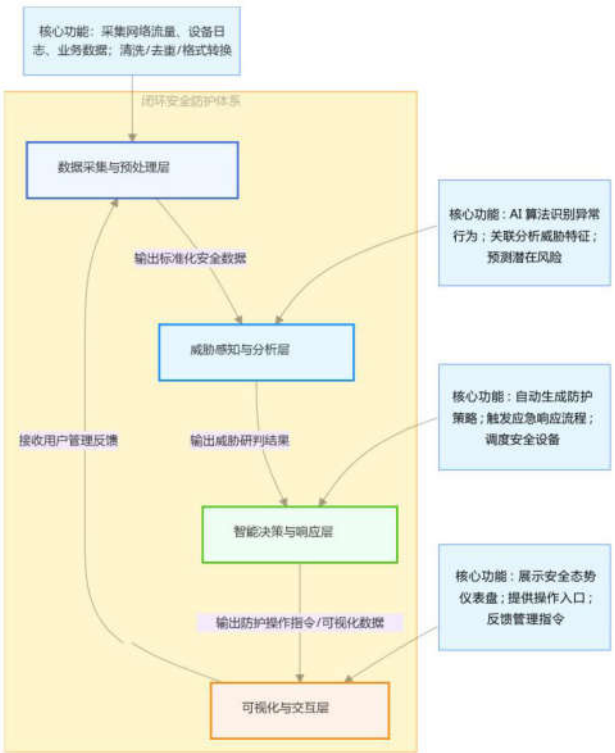

图1

2.2 数据采集与预处理层

数据采集与预处理层是人工智能应用于广播电视网络安全的基石。在广播电视网络中，数据来源广泛，涵

盖网络流量数据、设备日志、用户行为数据等。通过部署在网络各节点的传感器、探针等设备，实时收集这些多元数据。采集到的原始数据往往存在噪声、缺失值和重复信息等问题，预处理环节至关重要。它包括数据清洗，去除无效和错误数据；数据集成，将来自不同源的数据合并统一；数据变换，把数据转换为适合后续分析的格式，如将文本数据向量化。经过预处理，数据质量得到提升，为后续威胁感知与分析提供准确、完整的数据基础，确保人工智能模型能够基于可靠数据进行学习和决策，从而有效识别广播电视网络中的潜在安全风险。

2.3 威胁感知与分析层

威胁感知与分析层是人工智能在广播电视网络安全中的核心环节。该层利用机器学习、深度学习等算法，对采集并预处理后的数据进行深度挖掘。通过构建各类模型，如异常检测模型，可识别网络流量、用户行为中的异常模式，判断是否存在恶意攻击；分类模型能对不同类型的威胁进行精准分类，如区分是DDoS攻击还是恶意软件感染。同时，结合大数据分析技术，对海量数据进行关联分析，发现潜在的安全威胁趋势和规律。这一层能够实时、准确地感知广播电视网络中的各种威胁，为后续的智能决策与响应提供有力依据，帮助安全人员及时了解网络的安全状况。

2.4 智能决策与响应层

智能决策与响应层基于威胁感知与分析层的结果，运用人工智能技术实现自动化的决策与响应。当检测到安全威胁时，该层会根据预设的规则和算法，快速评估威胁的严重程度和影响范围，进而制定相应的应对策略。而对于严重的攻击行为，则会自动触发防护机制，如阻断网络连接、隔离受感染设备等。智能决策与响应层能够大幅提高安全响应的速度和效率，减少人工干预带来的延迟和误差，在威胁发生的瞬间及时采取行动，有效降低安全事件对广播电视网络造成的损害，保障网络的稳定运行。

2.5 可视化与交互层

可视化与交互层为用户提供了直观、便捷的安全管理界面。它将复杂的网络安全数据和信息以图表、报表、仪表盘等可视化形式呈现出来，使安全人员能够快速、清晰地了解广播电视网络的安全态势，包括威胁的分布、发展趋势等。同时，该层支持用户与系统进行交互，安全人员可以通过界面操作，对智能决策与响应层的策略进行调整和优化，如修改威胁检测的阈值、调整防护措施等。此外，可视化与交互层还具备报警功能，当出现严重安全威胁时，能及时向用户发出警报[2]。

3 人工智能在广播电视网络安全中的关键应用场景

3.1 智能威胁检测

（1）异常流量检测。在广播电视网络里，异常流量往往是安全威胁的先兆。人工智能借助机器学习算法，构建正常流量模型。它能实时分析网络流量的特征，像流量大小、频率、流向等。一旦实际流量偏离正常模型，就会判定为异常。这种检测方式高效准确，能及时发现潜在风险，为广播电视网络的稳定运行保驾护航，避免因流量异常导致的节目中断或数据泄露等问题。（2）恶意代码识别。广播电视网络中，恶意代码是严重威胁。人工智能通过深度学习，对大量已知恶意代码样本进行学习，提取其特征模式。当有新的文件或程序进入网络时，系统会将其特征与已学模式对比。若匹配度高，则判定为恶意代码。比如，用户上传的某个视频文件，经人工智能分析发现其包含可疑的代码结构，与已知的勒索软件特征相符，就会立即发出警报并阻止其传播。这种方式可快速精准识别恶意代码，防止其对广播电视网络系统和数据造成破坏。（3）APT攻击追踪。APT攻击具有长期性、隐蔽性，对广播电视网络安全威胁极大。人工智能利用大数据分析和关联技术，追踪APT攻击的各个环节。它通过分析网络日志、系统行为等数据，构建攻击链模型。当发现可疑行为时，沿着攻击链进行溯源分析。例如，从某个异常的登录行为入手，通过分析相关数据流量、系统操作记录等，逐步追踪到攻击源头和攻击路径。

3.2 自动化安全审计

（1）设备配置合规性检查。在广播电视网络中，众多设备的配置合规性至关重要。人工智能可依据预设的合规标准，自动扫描网络设备的配置信息。它能快速比对设备当前配置与标准配置的差异，精准识别出诸如端口设置不当、访问权限配置错误等违规情况。例如，对于核心交换机，若其访问控制列表配置有误，可能引发安全风险，人工智能系统能及时检测并发出警报，助力技术人员快速整改，保障设备安全稳定运行。（2）内容安全审核。广播电视内容的安全合规不容有失。人工智能借助自然语言处理和图像识别技术，对节目内容进行自动化审核。它能分析文本中的敏感词汇、违规表述，识别图像和视频中的不良信息、违规画面。比如，在直播节目中，若出现违反规定的言论或画面，人工智能系统可迅速捕捉并标记，及时通知审核人员处理，确保播出内容符合法律法规和社会道德规范，维护良好的传播环境。（3）供应链安全评估。广播电视网络的供应链涉及众多环节和供应商，其安全性影响整体网络。人工智

能可收集供应链各环节的数据，包括供应商资质、产品安全记录等。通过分析这些数据，评估供应链中潜在的安全风险，如供应商是否存在数据泄露历史、产品是否存在安全漏洞等。一旦发现风险，能及时提醒相关人员采取措施，如更换供应商或加强产品安全检测，保障广播电视网络供应链的安全可靠。

3.3 攻击面动态管理

（1）资产发现与分类。在广播电视网络复杂的环境中，准确发现并分类资产是攻击面动态管理的基础。人工智能利用网络探测、数据分析等技术，自动扫描并识别网络中的各类资产，如服务器、存储设备、终端等。依据资产的功能、重要性及安全需求进行细致分类，比如将承载核心业务的服务器归为关键资产。这有助于清晰掌握网络资产全景，为后续针对性地实施安全防护策略提供依据，有效缩小潜在攻击面。（2）漏洞优先级排序。广播电视网络存在大量设备和软件，漏洞不可避免。人工智能通过分析漏洞的严重程度、利用难度、影响范围等因素，结合资产的重要性和业务关联性，对漏洞进行优先级排序。例如，对于影响核心节目播出系统的严重漏洞，赋予高优先级，提醒安全人员优先修复。这种排序方式能合理分配安全资源，高效处理漏洞，降低被攻击的风险，保障网络的稳定运行。（3）零信任架构实施。零信任架构强调“默认不信任，始终验证”。人工智能在广播电视网络中实施零信任架构时，持续对用户、设备、应用的身份和行为进行验证。通过分析用户登录地点、操作习惯等数据，判断其合法性。这种动态验证机制能有效防止内部人员违规操作和外部攻击者入侵，持续缩小攻击面，为广播电视网络构建更安全可靠的环境。

3.4 应急响应与恢复

（1）攻击链重构。在广播电视网络遭遇攻击后，人工智能可借助大数据分析与关联技术，对攻击过程中的各类数据，如网络流量、系统日志等进行深度剖析。通过还原攻击步骤、识别攻击手段和工具，精准重构攻击链。这能帮助安全团队清晰了解攻击路径和目的，明确攻击者在网络中的活动轨迹，为后续的溯源、防范类似攻击提供关键依据，提升应急响应的针对性。（2）隔离与修复。人工智能驱动的应急系统能迅速识别受攻击的设备或系统部分。一旦发现攻击，可自动隔离受感染区域，防止攻击扩散至整个广播电视网络。同时，依据预先设定的修复策略和知识库，对受损系统进行快速修复。例如，自动下载并应用安全补丁、恢复被篡改的数据等，最大程度减少攻击造成的损失，使网络尽快恢复正常运行。（3）业务连续性保障。为保障广播电视业务在攻击后的连续性，人工智能会实时监测业务运行状态。当检测到业务因攻击受阻时，自动切换至备用资源或备份系统。比如，在直播业务受攻击中断时，快速启用备用直播线路和设备。

3.5 安全运营优化

（1）威胁情报聚合。人工智能能够对海量的威胁情报源进行自动聚合与整合。它可以收集来自行业报告、安全论坛、漏洞数据库等多渠道的威胁信息，通过自然语言处理和机器学习技术，提取关键威胁特征，如新型攻击手法、热门漏洞等。将这些分散的情报汇聚成全面、准确的威胁图景，为广播电视网络安全运营团队提供及时、有效的威胁预警，助力其提前制定应对策略，增强安全防御的前瞻性。（2）安全策略优化。基于威胁情报聚合的结果以及广播电视网络的实际安全状况，人工智能可对现有安全策略进行智能优化。它能分析安全策略的执行效果，识别出过于宽松或严格的部分。例如，根据新的攻击趋势调整防火墙规则、入侵检测系统的阈值等。通过持续优化安全策略，确保其与不断变化的安全威胁相匹配，提高安全防护的精准性和有效性，降低网络被攻击的风险。（3）人员技能提升。人工智能可助力广播电视网络安全人员技能提升。它能够提供个性化的培训方案，根据人员的技能水平和岗位需求，推荐相关的学习资料和模拟演练场景。通过虚拟攻击环境，让人员在实践中学习应对各类安全事件的方法[3]。

结束语

人工智能在广播电视网络安全领域的研究与应用，为行业带来了前所未有的变革与保障。通过智能威胁检测、自动化安全审计、攻击面动态管理等一系列创新应用，有效提升了广播电视网络应对安全威胁的能力，降低了安全风险，保障了业务的连续稳定运行。然而，技术的发展永无止境，未来仍需持续探索人工智能与广播电视网络安全的深度融合。相信随着研究的不断深入和实践的持续推进，人工智能将发挥更大作用，为广播电视网络安全构筑起更加坚固的防线，推动行业在数字化浪潮中稳健前行。

参考文献

[1]金昭延.人工智能技术赋能广播电视媒体的方向与路径[J].西部广播电视,2021,42(6):40-42.

[2]包崇正.数字广播电视宣传对于5G技术的运用[L].云南经济日报,2021,7(16):3.

[3]袁玉平.基于人工智能的广播电视内容监测系统[J].中国有线电视,2021,2(5):465-467.