物联网时代计算机信息技术在网络安全中的运用

王子虎
江西工程学院（智慧产业学院） 江西新余 338000

摘 要：随着物联网技术快速普及，各种智能终端设备相互连接形成了复杂的协作网络，这使得数据交换方式与通信架构变得越来越多样化。大量设备之间的频繁交互产生了海量数据流，对网络安全防护提出新的挑战。鉴于此，本文从计算机信息技术在网络安全中的重要性出发，重点分析基于人工智能分析流量、轻量加密、设备指纹识别与深度学习检测等技术路径，以期为构建更完善的网络安全体系提供新的思考方向。

关键词：物联网时代；计算机信息技术；网络安全

引言

近年来，计算机信息技术与人工智能、大数据分析、区块链等新兴技术相结合，为网络安全防护带来了新的突破。2023年《数字中国建设整体布局规划》特别强调，要加强保护关键信息基础设施及数据资源，提高网络安全防御能力，这充分说明技术创新在维护网络安全中的重要性。在物联网环境下，仅靠单一的安全措施已无法满足需求，必须构建多层次、协同联动的防御体系，才能有效应对各类复杂威胁，保障数据安全与网络环境的稳定运行。

一、计算机信息技术在网络安全中的重要性

（一）智能加密守护数据隐私

在物联网环境中，安全防护数据离不开智能加密技术。目前各类终端设备产生数据量急剧增长，传统的固定加密方式已难以满足实际需求，现代智能加密系统采用动态调整策略，能够根据不同的应用场景自动选择合适的加密强度。这种灵活性既保证了关键数据的安全，又避免了过度加密造成资源浪费。动态加密机制可实时监测网络环境变化，当检测到潜在风险时，系统会立即提升特定数据流的保护级别。此主动防御方式特别适合物联网场景，因为物联网设备通常计算能力有限，需要兼顾安全性与运行效率。除此之外，智能加密不但保护静态存储的数据，更重要的是确保数据在传输过程中的安全。从终端设备到云端服务器，能严密保护每个环节[1]。最新的加密算法还能识别异常访问行为，自动触发额外的验证流程，有效提高黑客攻击的难度。

（二）动态认证阻断非法入侵

物联网安全防护体系中，面对日益增多的设备接入请求与数据交换行为，传统的固定密码验证方式已显得力不从心。动态认证用多因素验证手段，有机结合用户身份核验与当前网络状况、设备运行状态等要素，大幅提高了系统的安全防护水平。并且若系统检测到异常登录尝试时，会自动增加验证步骤，要求用户提供更多身份证明。此外，动态认证的实施显著改善网络边界防护效果，黑客即便获取了部分认证信息也难以通过后续的实时验证环节。同时，由于认证强度会根据风险等级动态调整，既保证了高安全性，又避免了不必要的验证负担[2]。

（三）边缘计算强化终端防护

边缘计算明显增强物联网终端的防护能力，在靠近设备的地方就能处理数据，这样可以在传输过程中减少暴露风险，减少被攻击的机会。边缘节点具备本地计算与判断功能，安全防护措施能够在第一时间作出反应，不再需要依赖远程中心的统一调度，因此响应速度更快，实时防护能力更强。在数据传送之前，边缘设备已筛查信息，把未经授权的访问以及恶意行为拦截在外，有效降低泄露数据的概率。边缘计算让网络防线既有物理分布，又具备逻辑隔离，让安全体系从传统的集中模式向多层联动转变，让终端防护慢慢完成由被动抵御向主动应对转型。

（四）流量画像精准识别威胁

流量画像技术在物联网网络安全领域的应用价值

作者简介：王子虎（1988.07-）男，汉族，安徽利辛人，硕士，讲师，研究方向：人工智能、大数据、物联网通信。

日益凸显，不同设备、应用与用户在网络中的行为模式各具特征，这些特征汇聚成完整的流量画像，为威胁识别提供了高精度依据。系统经过长期观测流量特征，能够构建稳定的基线模型，用于对比当前网络活动与预期模式的偏离情况[3]。微小异常变化均可及时捕获，使潜伏型威胁与渐进式攻击无所遁形。另外，流量画像赋予安全防护体系更强的细粒度感知能力，帮助识别零日漏洞利用、横向渗透等复杂威胁形式，显著提升预警时效性。网络中每一次访问请求、数据传输及指令执行均受到严密监控，保障数据在交换和处理过程中的完整性。依托流量画像，网络安全防护能力达到质的跃升，防御策略不再停留于规则匹配，而是迈向智能识别行为特征新阶段。

二、物联网时代计算机信息技术在网络安全中的应用

（一）基于AI流量分析，实时阻断DDoS攻击

在物联网环境中DDoS攻击防护面临新的挑战，传统方法难以应对海量设备产生的复杂流量，而人工智能技术为解决这个问题提供新思路。智能流量分析系统能够持续学习网络行为特征，建立动态的流量基准，此系统不依赖固定规则，而是经过分析流量模式、连接频率等特征自动识别异常。当网络中出现异常流量时，系统能快速判断是否属于攻击行为，并及时触发防护机制。相比传统方法，这种智能分析可以更准确地发现隐蔽的攻击，减少误判情况。由于物联网设备种类繁多，网络环境复杂，自适应能力显得尤为重要。系统还能根据历史数据不断优化判断标准，保持防护效果。

具体实施时，安全团队需要先规划流量监测点，在网络入口、核心交换区等关键位置部署探针。目前某企业网络入口部署探针8个，核心交换区部署探针12个。这些监测点会收集流量大小、数据包特征、访问频率等信息，例如高峰期单点监测流量达837.46MB，日均捕获异常数据包约1264.30个。收集到的原始数据需要经过清洗及标准化处理去除无效信息并提取关键特征，然后由采用分布式架构的分析系统先进行初步分析，以此减轻中心服务器的压力。安全工程师会准备大量真实的网络流量数据，包括正常流量和攻击流量，用于训练分析模型。当前训练集包含正常样本约350000条，攻击样本约96500条。训练过程中应不断调整参数，使模型能够准确区分正常访问与攻击行为。系统上线后，运维人员要实时监控分析结果，当发现异常流量时，立即检查系统判断是否准确。同时，防护策略会根据攻击特征动态调整，确保既能有效拦截攻击，又不影响正常业务（如表1所示）。

表1　网络安全监测实施表

监测点类型	部署数量	监测指标	数据量/样本数	处理方式	系统性能
网络入口	8个	流量大小	高峰期837.46MB	数据清洗及标准化	响应时间0.34s
核心交换区	12个	异常数据包	日均1264.30个	分布式架构分析	–
训练数据集	–	正常样本	350000条	模型训练	–
训练数据集	–	攻击样本	96500条	参数调整	–

（二）利用轻量加密算法，保障终端通信安全

在物联网环境下，终端设备往往体积小、功耗低、运算资源有限，因此传统加密方式在实际应用中难以兼顾安全性与性能。轻量加密算法正是针对这些设备的特点进行设计的，它在保障通信安全的同时，降低硬件资源消耗的情况。这类算法重点优化运算步骤，使加密解密过程更加高效，减少不必要的计算负担。密钥长度合理、运算逻辑精简，有效保护数据传输中的机密性，能防止数据窃取或篡改。在物联网网络架构中，轻量加密算法适用于多种协议以及不同通信场景，不会因为设备性能差异而产生适配障碍。实际应用时，轻量加密机制让数据封装更严密，不易被非法截获。算法结构灵活，嵌入各类硬件环境都具备较高兼容性，并能在保障数据安全的同时减少网络带宽压力。

（三）采用设备指纹技术，精准识别非法接入

物联网环境下，传统设备识别身份方式容易出现仿冒，难以应对复杂的网络环境。设备指纹技术能让每台联网设备都具有独特的硬件特征，就像人的指纹一样。技术人员需要收集设备的MAC地址、CPU序列号、操作系统版本等几十项参数，为每台设备建立专属的数字指纹。这种方法不需要额外硬件支持，也不会影响设备正常使用。当设备尝试接入网络时，系统会将其特征比对预存的指纹数据库，快速判断设备身份是否合法。由于物联网设备数量庞大且类型复杂，传统认证方式管理成

本过高，但是技术特别适合物联网场景。此外，当某个设备的网络通信模式突然改变时，指纹识别会自动提高警惕等级。

部署设备指纹系统需要多个技术团队协作，先由网络工程师确定需要采集的设备特征参数，这些参数要具有唯一性且不易被伪造，常见的选择包括网卡信息、固件版本、时钟偏差等物理特征。目前系统共设置采集参数12项，覆盖设备总数达38672.00台。软件开发人员随后应编写特征采集程序，这个程序要足够轻量，不能影响设备性能，程序平均运行资源占用为1.84%。测试人员可在不同品牌、型号的设备上反复测试，确保采集程序兼容性良好，当前累计完成测试设备192种（unit：types），兼容成功率达到98.26%（unit：percent）。数据库团队负责设计指纹存储方案，采用分布式架构来应对海量设备数据，目前已部署分布式节点32个（unit：nodes），单节点最大存储容量为2.50TB（unit：terabytes）。安全专家需要制定指纹更新策略，因为设备软件升级可能导致特征变化。

（四）运用深度学习模型，智能检测零日漏洞

深度学习技术具备强大的提取数据特征能力，能够更精准地捕捉隐藏在海量数据中的异常行为。物联网场景下设备数量多、网络结构杂、数据交互频繁，传统规则或特征库匹配检测方法在面对未知漏洞和新型攻击时显得力不从心。深度学习模型依靠训练获得的适应能力，可以从流量数据、日志信息、系统调用等多维数据中挖掘潜在威胁，提升发现未知攻击的能力。模型利用多层网络结构深入分析数据，既关注流量表面特征，又能识别复杂交互背后的微观行为差异。此外，时序特性与多维指标数据的结合帮助模型更好地理解攻击行为的时空特征，进而提高检测的准确率。

在实际落地过程中，团队需要分工协作推进各项工作。数据工程人员要在关键位置部署采集设备，实时抓取通信流量、会话数据和日志记录，目前已布设采集点54个，日均采集原始数据量达186.75GB，为训练模型积累数据基础。数据预处理阶段，特征工程师需要对这些原始数据做格式转换、标准化和特征提取，去掉干扰信息，筛选对检测有用的数据特征，当前每批次处理数据样本为100000.00条，平均预处理时长为14.20分钟。接着，建模人员可根据物联网流量特征设计模型结构，一般会结合卷积、循环、注意力等层次以增强识别空间特性的能力，现有模型结构共包含17层，参数量约为3.45M。训练阶段由算法工程师调优超参数，利用分布式训练缩短训练耗时，提升训练效率，目前训练周期为8.25小时，在4台GPU设备上并行完成。模型成型后，开发人员会把它打包成检测服务接口，在安全网关、流量镜像点等位置布署检测功能，以支持边缘设备上的实时检测任务。运维人员应结合检测结果设置告警机制以及拦截策略，让风险能快速隔离并响应，减少潜在危害。当前平均每日拦截异常行为约2436.50次。同时，监控组会用可视化工具跟踪检测状态、拦截记录，方便技术人员掌握系统运行情况，系统仪表盘刷新频率为30.00秒/次。

结束语

物联网安全防护正在经历快速变革，各类终端设备在数据交换中构建出更加复杂多样的网络体系，使计算机信息技术与防护架构深度融合。智能算法在识别风险、实时监测以及应急处理等环节展现出高效协同的优势，技术应用逐渐从局部防护向覆盖全流程的综合防御发展。未来的防护方案应加强多层防御体系与边缘智能的协作效能，提升数据传输管理、信息加密及动态身份验证等功能的配合水平，进而更好地应对物联网环境中持续出现的新型安全威胁。

参考文献

[1]李馨，李荣波.试论数据挖掘技术在计算机网络信息风险防范中的应用[J].中国宽带，2025，21（07）：34-36.

[2]齐歌.大数据技术在计算机网络信息安全管理中的应用[J].中国宽带，2025，21（05）：40-42.

[3]李宪伟，陈静.基于计算机网络技术的网络信息安全防护体系建设[J].长江信息通信，2025，38（04）：144-146.