信息工程在网络安全与信息化融合中的应用

王晶晶
鹿邑县平安建设促进中心　河南　周口　466000

摘　要：信息工程是推动网络安全与信息化深度融合的核心支撑，能够破解传统网络安全防护的局限，强化融合过程中的安全管控能力。结合信息工程技术特性，从技术架构、深度学习应用、态势感知与融合模型、多层次防护策略四个维度，系统梳理信息工程在融合中的具体应用要点，完善安全防护体系与技术路径。本文通过整合技术架构搭建、智能研判、态势感知与分层防护等核心内容，构建全方位的融合应用体系，有效提升网络安全防护的精准性与高效性，为网络安全与信息化融合实践提供实操支撑。

关键词：信息工程；网络安全；信息化融合；态势感知；多层次防护

引言：网络安全与信息化融合是数字时代发展的必然趋势，二者协同推进能够提升信息系统的运行效率与安全水平，而信息工程为二者深度融合提供关键技术支撑。当前网络环境日趋复杂，安全威胁呈现多元化、智能化特征，传统安全防护模式难以适配融合发展需求，存在防护滞后、研判不精准等问题。梳理信息工程在融合中的应用路径，完善技术架构与防护策略，破解融合过程中的安全难题，对推动网络安全与信息化高质量融合具有重要现实意义。

1 信息工程与网络安全融合的技术架构

1.1 信息网络的层次化体系结构

信息网络层次化体系结构以OSI七层模型与TCP/IP四层模型为基础框架，按功能维度划分为物理层、数据链路层、网络层、传输层与应用层，各层边界清晰且功能独立[1]。物理层聚焦信号传输与介质适配，为上层提供稳定的物理链路支撑；数据链路层实现帧封装与差错校验，保障数据帧的可靠传递；网络层负责路由寻址与路径规划，完成跨网段数据转发；传输层提供端到端数据传输控制，平衡传输可靠性与实时性需求；应用层对接各类业务场景，承载数据交互与服务供给功能。

1.2 资源子网与通信子网的协同机制

资源子网与通信子网的协同机制是架构高效运行的关键支撑，明确两类子网的功能定位与交互逻辑，实现资源调度与数据传输的动态匹配。资源子网涵盖计算设备、存储单元与终端节点，承担数据处理、资源存储与业务服务供给功能，负责本地资源的安全管控与调度分配；通信子网包含传输介质、交换设备与路由节点，专注数据转发、链路维护与通信质量保障，构建稳定的数据传输通道。协同机制通过标准化接口实现两类子网的数据交互与指令传递，资源子网依据业务需求向通信子网发起数据传输请求，通信子网结合网络状态优化传输路径，双方实时同步安全运行信息，形成资源管理与通信安全的联动响应，保障数据流转全程可控。

1.3 网络协议与分层设计原则

网络协议与分层设计原则贯穿架构设计全流程，以标准化协议体系支撑层次化功能落地，保障不同模块与设备间的兼容互操作。分层设计遵循功能独立、单向依赖与接口标准化核心准则，各层仅向上层提供专属服务，同时调用下层基础能力，层间交互通过统一接口完成，降低跨层交互复杂度。网络协议作为各层功能实现的核心规则，物理层与数据链路层采用介质访问控制协议保障链路稳定，网络层依托IP协议实现路由寻址，传输层通过TCP/UDP协议适配不同传输需求，应用层部署HTTP、FTP等协议支撑业务交互。协议体系与分层架构深度适配，既保障网络通信的规范性，又为协议安全检测与防护提供标准化依据，支撑安全机制与协议栈的融合部署。

1.4 多源异构数据驱动的安全检测架构

多源异构数据驱动的安全检测架构以数据融合与特征解析为核心，整合网络流量、设备运行、系统日志等多维度异构数据，构建全域覆盖的安全检测体系。架构采用分布式数据采集与集中式分析处理相结合的模式，部署多节点采集模块，适配不同格式、不同来源数据的接入需求，完成数据的初步清洗与归一化处理。核心分析模块基于特征匹配与异常识别技术，挖掘多源数据中的安全关联特征，识别网络攻击、数据泄露等异常行为，覆盖协议异常、流量突变、非法访问等多类安全风险。架构支持检测策略的动态更新与模块弹性扩展，适配异构数据类型与安全威胁的迭代变化，实现安全检测的精准化与实时化，为网络安全防护提供数据支撑与决

策依据。

2 深度学习在网络安全中的融合应用

2.1 静态特征与动态行为的联合分析

静态特征与动态行为的联合分析拓宽网络安全研判的分析维度，补齐单一研判模式存在的分析盲区。静态特征侧重抓取网络程序代码结构端口运行状态系统配置信息等固定化信息内容，完成基础层面的安全基础判定[2]。动态行为聚焦网络数据传输走向节点访问轨迹业务交互模式等持续变化的运行状态，捕捉网络运行流程里出现的异常走向。

2.2 自适应安全防御架构的构建

自适应安全防御架构依托深度学习具备的自主学习能力搭建而成，能够顺应网络运行环境的变化做出自主调整。架构摒弃固定不变的防护设置，依托持续积累的网络运行数据完成自主学习迭代，主动适配不同网络运行场景下的防护需求。架构内部划分多层级防护运行模块，依靠算法完成模块之间的联动调配，依照网络整体运行态势调整防护资源排布形式。借助自主学习积累的海量网络运行规律，架构可以自主调整防护运行逻辑，弱化外界环境变动对安全防护工作造成的干扰，维持网络防护体系长久稳定运转。

2.3 多源异构数据融合的安全检测系统

多源异构数据融合的安全检测系统依托深度学习完成不同类别网络数据的整合梳理工作，拓宽安全检测覆盖范围。系统收纳网络流量信息设备运行日志业务交互数据等不同形式的信息资源，对零散分布的原始数据开展统一规整梳理。借助算法完成不同维度数据信息的关联梳理，挖掘零散数据内部潜藏的安全关联信息，梳理数据之间存在的内在联系。系统依托整合完成的完整数据信息开展安全筛查工作，拓宽安全检测的覆盖范围，提升网络异常状态筛查的全面程度，夯实智能安全检测的数据基础。

2.4 深度学习模型在威胁识别中的嵌入方式

深度学习模型在威胁识别环节拥有多样合理的嵌入形式，能够贴合不同网络防护场景完成灵活布设。可将模型布设至网络前端数据接入环节，在数据进入网络体系之初完成基础威胁筛查工作，提前拦截浅层网络风险。也可将模型融入后台数据研判中心，对汇总完成的全网运行数据开展深度解析，深挖隐藏程度较深的网络威胁。还可将模型布设至终端运行节点，贴近业务运行场景完成局部区域的安全研判。多样化的嵌入形式能够贴合不同层级网络安全防护需求，让智能识别能力渗透至网络运行各个环节，完善全网范围的威胁识别布局。

3 网络安全态势感知与信息融合模型

3.1 JDL数据融合模型的四级处理架构

JDL数据融合模型的四级处理架构，是网络安全态势感知中数据整合与解析的核心框架，按数据处理流程划分为数据级、特征级、决策级与态势级四个递进层级[3]。数据级处理聚焦原始数据的采集与预处理，完成多源数据的清洗、去重与归一化，统一数据格式以适配后续处理需求。特征级处理提取各类数据的核心特征，通过特征映射与筛选，保留与安全态势相关的关键信息，降低数据处理冗余。决策级处理对特征信息进行关联分析，结合安全规则完成初步研判，输出各类安全事件的判定结果。态势级处理整合前三级处理结果，提炼网络安全整体运行态势，形成全面的态势描述，为后续态势评估与预测提供基础支撑。

3.2 网络安全态势评估的数学方法

网络安全态势评估的数学方法为态势量化分析提供科学工具，通过量化指标与数学建模实现态势的精准描述。层次分析法将复杂态势评估拆解为多个层级的指标体系，通过指标权重分配实现多维度态势的综合研判。贝叶斯估计法依托概率统计理论，结合历史数据与实时数据，推算安全态势的演变概率，提升评估结果的可靠性，适配动态变化的网络环境。

3.3 基于统计的态势分析方法

基于统计的态势分析方法以数据统计规律为核心，通过挖掘海量网络运行数据的统计特征，识别安全态势的变化规律。该方法依托概率统计、回归分析等技术，对网络流量、日志数据等进行统计建模，提取数据的均值、方差、异常频次等统计指标。通过分析统计指标的变化趋势，捕捉网络运行中的异常波动，识别潜在安全威胁。方法注重数据积累与规律总结，能够通过历史统计数据预判态势演变趋势，为态势感知提供数据驱动的分析支撑，适配大规模网络的态势研判需求。

3.4 面向大型信息系统的态势预测模型

面向大型信息系统的态势预测模型聚焦大规模网络的动态性与复杂性，实现安全态势的前瞻性研判。模型整合网络运行数据、历史威胁数据与环境参数，依托时序分析、深度学习等技术构建预测模型。通过分析态势演变的时间序列规律，捕捉态势变化的内在关联，预判未来一段时间内的网络安全态势。模型具备良好的扩展性与适配性，能够应对大型信息系统中多节点、多业务的复杂场景，及时预判潜在安全风险，为安全防护决策提供前瞻性支撑。

4 网络安全的多层次防护策略

4.1 防静电、防雷击、防电磁泄漏

物理安全层是网络安全防护的基础屏障，聚焦网络硬件设施与运行环境的安全防护，重点落实防静电、防雷击、防电磁泄漏三项核心措施。防静电通过部署防静电地板、佩戴防静电装备、优化环境湿度控制，抑制静电产生与积累，避免静电击穿电子设备元器件、破坏设备运行稳定性[4]。防雷击通过安装防雷装置、规范接地系统，引导雷电电流安全泄放，阻隔雷电冲击对网络设备、传输线路造成的损坏，保障硬件设施正常运行。防电磁泄漏通过采用电磁屏蔽材料、优化设备布局，阻断网络设备运行过程中产生的电磁信号泄露，防止敏感信息被非法截取，筑牢网络安全的物理防线。

4.2 口令密码与权限控制

逻辑安全层聚焦网络访问的合法性管控，通过口令密码与权限控制构建访问安全屏障，防范非法访问与权限滥用。口令密码管理需规范密码设置标准，要求密码具备足够复杂度，定期进行密码更新与更换，采用加密存储方式保护密码信息，避免密码泄露导致非法访问。权限控制需依据业务需求划分访问权限，明确不同岗位的访问范围与操作权限，落实权限最小化原则，限制无关人员对敏感数据与核心系统的访问，通过权限校验与访问审计，追踪访问行为，及时发现权限滥用问题。

4.3 漏洞修复与用户权限管理

操作系统安全层是网络安全防护的核心环节，通过漏洞修复与用户权限管理防范系统层面的安全风险。漏洞修复需建立常态化漏洞扫描机制，及时发现操作系统自身存在的安全漏洞与潜在隐患，针对性安装漏洞补丁，填补安全漏洞，避免黑客利用漏洞入侵系统、窃取数据。用户权限管理需梳理系统用户清单，清理无效用户与冗余权限，规范用户账户创建、注销流程，明确各类用户的操作权限，禁止普通用户获取管理员权限，通过用户行为监控，防范恶意操作对操作系统造成的破坏。

4.4 通信安全与数据完整性保障

联网安全层聚焦网络通信过程的安全管控，重点保障通信安全与数据完整性，防范数据传输过程中的泄露与篡改。通信安全通过采用加密通信协议，对传输数据进行加密处理，阻隔非法拦截与窃听，确保数据在传输过程中的保密性。数据完整性保障通过部署校验机制，对传输前后的数据进行校验比对，识别数据传输过程中出现的篡改、丢失等问题，及时进行数据恢复与修正，采用数据校验码、哈希算法等技术，确保传输数据的真实性与完整性，保障网络通信安全有序。

4.5 加密传输与备份恢复机制

数据安全层聚焦核心数据的安全保护，通过加密传输与备份恢复机制，实现数据全生命周期的安全管控。加密传输对各类敏感数据、核心数据进行加密处理，无论是存储还是传输过程，均采用符合安全标准的加密算法，防止数据被非法窃取与泄露[5]。备份恢复机制需建立常态化数据备份流程，定期对核心数据进行备份，选择安全可靠的备份存储介质，明确备份频率与备份策略，同时完善数据恢复流程，确保数据丢失、损坏时，能够快速完成数据恢复，减少数据安全事件造成的损失。

结束语

信息工程为网络安全与信息化融合提供坚实技术支撑，二者深度融合能够破解传统网络安全防护短板，提升信息系统运行的安全性与高效性。全文从技术架构、深度学习应用、态势感知与融合模型、多层次防护策略四个核心维度，梳理信息工程在融合中的具体应用，构建起全方位、全流程的安全融合体系。通过完善技术架构、强化智能研判、精准感知态势、落实分层防护，能够有效防范各类网络安全威胁，保障网络安全与信息化融合有序推进，为数字时代网络安全保障提供可靠支撑。

参考文献

[1]李晨瑶.信息工程在网络安全与信息化融合中的应用[J].网络安全和信息化,2025(9):136-138.

[2]刘梦瑶,穆媛媛,李国印.信息工程环境下数据技术对网络安全的影响分析[J].网络安全和信息化,2025(6):133-135.

[3]李国印,刘梦瑶,穆媛媛.网络安全事件响应流程在信息工程中的优化研究[J].网络安全和信息化,2025(4):128-130.

[4]穆媛媛,李国印,刘梦瑶.基于信息工程技术的网络安全漏洞检测与修复研究[J].网络安全和信息化,2025(5):128-130.

[5]冯云婷,李攀,李景景,等.电子信息工程中网络安全技术应用研究[J].软件,2025,46(2):4-6.