文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

智慧城市网络安全架构中的基础设施保护策略

范彬彬
凯易讯网络技术开发（南京）有限公司
DOI:10.12238/acair.v3i1.11861

[摘　要] 智慧城市是新型城市化发展的重要方向,其网络安全体系直接关系到关键基础设施的运行稳定性和城市服务的连续性。如何在多变的安全环境中构建全面、高效的保护策略是智慧城市网络安全的重要研究内容。本文围绕智慧城市网络安全架构,提出人工智能驱动的威胁检测响应、数据加密分布式存储、动态访问控制身份认证优化、物联网设备智能化安全防护及多主体协作安全态势感知五大策略,详细阐述各技术的实现方法和应用场景,从系统设计、技术融合和协作机制角度构建智慧城市的全方位安全防护体系,为复杂网络环境下的关键基础设施提供创新性的解决方案。
[关键词] 智慧城市；网络安全；人工智能；关键基础设施；物联网
中图分类号：TP18　文献标识码：A

Key Strategies for Critical Infrastructure Protection in Smart City Cybersecurity Architectures

Binbin Fan
Calix Network Technology Development (Nanjing) Co., Ltd.

[Abstract] Smart cities are a significant direction in modern urbanization, with their cybersecurity frameworks directly influencing the operational stability of critical infrastructure and the continuity of urban services. Developing comprehensive and efficient protection strategies in response to dynamic security challenges is a key research focus for smart city cybersecurity. This paper examines the cybersecurity architecture of smart cities and proposes five strategies: AI-driven threat detection and response, encrypted distributed data storage, dynamic access control with optimized identity authentication, intelligent security protection for IoT devices, and multi-agent collaborative security situational awareness. Each strategy is analyzed in detail, focusing on implementation methods and application scenarios. From the perspectives of system design, technological integration, and collaborative mechanisms, the paper constructs a comprehensive security framework for smart cities, providing innovative solutions for protecting critical infrastructure in complex network environments.
[Key words] Smart City; Cybersecurity; Artificial Intelligence; Critical Infrastructure Internet of Things (IoT)

引言

智慧城市建设依托信息技术的深度融合和关键基础设施的高效运行,但伴随城市数字化程度的提高,网络安全风险呈现出复杂化、多样化趋势[1]。关键基础设施作为城市运行的核心,其高度依赖网络互联的特性使其成为潜在攻击的重点目标,面临数据泄露、系统入侵、服务中断等诸多挑战。传统的安全防护手段由于响应速度慢、适应性弱,难以应对智慧城市复杂网络环境中的动态威胁。人工智能技术的引入为关键基础设施的网络安全提供全新路径,借助智能算法实现威胁识别、动态响应和实时防护,显著提升安全防御能力[2]。本文围绕智慧城市网络安全架构,重点研究关键基础设施的保护策略,借助技术创新全面提升关键基础设施的安全水平,为智慧城市的可持续发展提供坚实保障。

1 智慧城市网络安全架构概述

智慧城市网络安全架构需要满足关键基础设施的高效运行和安全防护需求,如图1所示,其拓扑结构展示互联网核心区、政务外网核心区和数据交换区的功能分布,各区域间利用逻辑隔离和专用通道实现安全通信[3]。底层架构由虚拟化区、物理主机区和开发测试池组成,提供计算和存储资源的稳定支撑,结合VXLAN与VLAN技术实现动态资源调度和网络隔离。人工智能技术贯穿全架构,利用智能决策、态势感知与威胁情报提升安全策略的响应速度与精准度,同时整合物联网安全、云计算安全与身份管理技术,形成高效协同的多层次安全防护体系,为智慧城市运行中的复杂网络环境提供技术支撑。

2 关键基础设施保护策略

2.1 AI驱动威胁检测响应

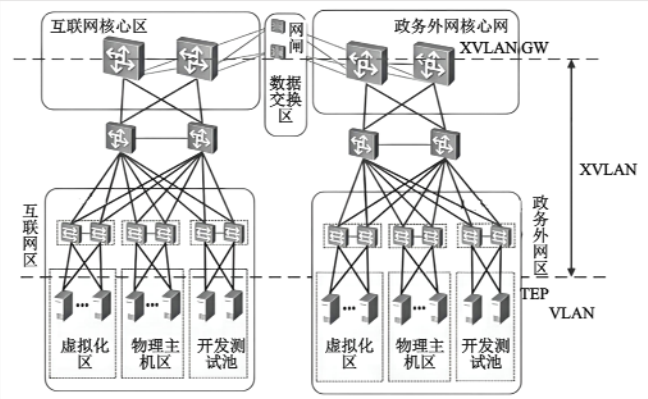

图1 智慧城市网络安全架构

智慧城市关键基础设施的威胁检测响应体系基于人工智能(AI)技术,在电网调度、交通信号控制和水务调度等场景部署精准的解决方案。电网调度系统在变电站和调度中心设置流量行为分析模型,采集设备通信数据和网络流量,结合历史日志构建基线模型,异常检测算法动态识别流量偏离情况,边缘节点生成警报并同步至云端系统。交通信号控制中,边缘节点结合卷积神经网络(CNN)分析实时视频流,提取交通流量特征,核查信号切换逻辑与交通数据是否匹配,限制异常指令执行并记录相关日志[4]。水务调度系统利用管网传感器采集流量、压力和调度数据,时序分析算法检测运行异常,规则库识别潜在管道故障或异常指令,触发警报并暂停异常指令传输。分布式检测架构中,边缘节点负责本地异常识别,云平台汇总节点结果生成全局威胁图谱,评估攻击路径和风险区域。在威胁响应中,动态权限管理机制对异常区域执行权限限制,对高风险设备进行隔离,减少敏感操作暴露,同时调整全局防护策略以应对威胁变化。

2.2数据加密分布式存储

分布式存储体系在智慧城市关键基础设施中,以数据分段加密、动态密钥管理和分布式节点协作为核心策略,将存储节点部署在电网调度中心、交通控制系统和医疗数据平台等子系统。数据存储时,分段算法将原始信息拆分为多个加密片段,每段由硬件安全模块(HSM)生成的独立密钥加密后分发至不同节点。链路加密技术贯穿数据传输全程,节点间的通信日志记录传输路径与加密状态并同步至云端监控平台支持状态审计。存储节点采用强一致性协议实现主存节点与从存节点的实时同步,确保数据完整性。访问控制模块借助多级权限验证策略限制用户访问,访问请求通过网关转发至目标节点,节点结合用户身份、设备指纹及操作环境核验权限,高敏感性数据经过多因子认证流程完成实时合法性判断。解密过程在目标节点完成,解密片段发送至访问网关后重组并验证完整性,再传输至用户终端。节点状态监测与验证由云端平台实时进行,异常行为或节点故障触发隔离策略,锁定访问路径并阻止异常操作。日志管理模块归档所有操作记录,为后续的溯源审计分析提供支持,保障分布式存储体系的高效协作与安全运行[5]。

2.3动态访问控制身份认证优化

基于事件流分析技术,利用时序行为建模动态捕捉用户访问模式的变化,将权限管理从传统静态规则切换为实时动态配置。用户每次访问请求均触发行为特征匹配流程,边缘节点通过嵌入轻量化AI模型,将用户操作特征与设备信任等级、当前环境参数进行关联计算,生成独立的访问凭据。访问凭据有效期与操作任务相关联,仅适用于当前任务范围,凭据过期后需重新生成,避免长期固定权限导致的安全风险。身份认证框架利用多域分布式验证技术,将用户认证任务分发至不同功能域内的验证节点,各节点独立处理特定维度的认证数据,生物特征验证由中心节点处理,同时认证结果借助聚合算法综合评估以实现分布式协同认证[5]。数据同步阶段,访问路径生成引擎将用户行为建模结果注入动态加密机制,为每个通信会话生成一次性加密密钥,密钥仅存储于信任硬件模块中,不在系统间传播。多级权限细化管理策略结合预测模型运行,分析用户的潜在访问需求与任务目标,对权限范围进行预生成,遇突发请求时权限调整的决策效率得到显著提升。系统日志管理模块引入智能签名追踪机制,所有访问凭据和认证记录均带有独立签名标识,分布式存储于区块链网络中,每次访问均可快速定位关联操作节点并溯源操作来源。系统内部设置动态协作规则优化模块,结合强化学习技术,模拟环境下的操作验证不断迭代权限分配策略,为关键基础设施提供灵活、精准且高效的动态访问控制解决方案。

2.4物联网设备智能化安全防护

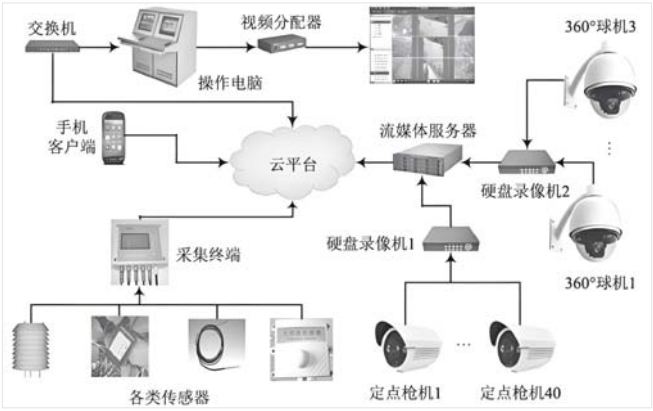

图2 智慧城市关键基础设施物联网设备安全防护架构图

物联网设备在智慧城市关键基础设施中的智能化安全防护需依托清晰的链路设计和分区策略。如图2所示的架构中,各类传感器、摄像设备和采集终端利用数据链路连接至流媒体服务器和云平台,形成分层式数据传输与处理体系。设备接入时,生成唯一身份标识并以加密形式记录在链上,注册请求在多个分布式节点之间通过共识机制验证。运行阶段,采集终端作为边缘节点,监控摄像头和传感器的操作日志与数据流。异常检测模型对设备行为偏离基线的操作生成警报,触发自动隔离机制,同时将状态同步至云平台。通信链路中,每次传输会话均采用一次性密钥进行动态加密,密钥由硬件模块生成且不在通信中明文传输。高风险设备的数据流在流媒体服务器中设置多层权限,未经授权的请求被实时拒绝并记录到日志。溯源策略根据攻击行为

特征和通信路径生成完整的攻击图谱,云平台基于溯源结果触发跨节点防护,限制攻击范围。设备退役时,使用区块链智能合约完成身份注销与数据清理,销毁过程记录在链上以供后续验证,防止设备被重新激活或利用[6]。

2.5多主体协作安全态势感知

依托分布式架构和智能技术,由政府、企业和公共设施管理方等主体共同参与,构建跨域数据共享与动态分析网络。每个主体的数据节点通过分布式共享网络连接,数据流、访问权限和操作日志以区块链技术加密存储,节点间的共识机制保障数据流转的完整性和可追溯性。态势感知引擎结合多模态数据处理与图神经网络(GNN),统一对各主体的数据进行建模,动态生成全局威胁图谱并识别潜在高风险区域。边缘计算节点负责本地数据的采集与初步分析,云平台通过整合边缘节点数据对全局态势进行建模与优化,实时调整资源分配策略。协作决策由智能合约模块驱动,各主体间的数据共享规则和响应任务通过合约执行,当检测到异常时,系统自动分配协同防护任务并触发跨主体资源部署。威胁情报共享采用联邦学习模型,在各主体间共享威胁特征参数,同时避免泄漏原始数据。针对复杂攻击场景,强化学习驱动的协作引擎进行模拟训练,优化任务分配与防御调整策略[7]。态势可视化系统结合增强现实技术,将动态威胁图谱与防护状态直观呈现,标注高风险区域及实时资源分布,辅助各主体协同完成安全防护任务。

3 结束语

智慧城市的网络安全架构是其可持续发展的重要基石,而关键基础设施的安全防护策略直接关系到城市运行的稳定性与可靠性。本文从五个方面系统性地探讨智慧城市网络安全的关键技术与实施路径。随着智慧城市应用场景的进一步扩展,网络威胁形式将更加复杂,对安全策略的智能化、动态性和协作性的要求也将不断提高,安全架构的持续优化和技术创新仍需深入探索与实践。

[参考文献]

[1]韦鸿流.智慧城市云平台网络架构研究[J].中文科技期刊数据库(引文版)工程技术,2024(12):077-080.

[2]郭占杰.人工智能在智慧城市中的应用过程[J].自动化与仪表,2024,39(9):162-164.

[3]宋豪杰,刘铭,查鹏皓,等.面向智慧城市的网络信息安全管理平台建设研究[J].项目管理技术,2024,22(10):122-128.

[4]王仕杰,邓智文.基于CNN和STM32的智慧城市环保净化车设计[J].中国科技期刊数据库工业A,2024(12):075-078.

[5]宋智明,余益民,王贵文,等.基于区块链智能合约的数字身份可验证凭证零知识认证和管理架构[J].信息安全学报,2023,8(1):55-77.

[6]尹建标,张言,史培中,等.面向工业物联网的策略隐藏属性基加密方案[J].现代电子技术,2025,48(1):90-96.

[7]王明程,王高开,李勇男.基于大模型智能体的安全风险态势感知框架构建[J].情报理论与实践,2024,47(7):190-198.

作者简介：

范彬彬(1986--),男,汉族,江苏通州人,本科,研究方向：计算机网络通信技术。