 DOI: https://doi.org/10.12349/iser.v7i5.10531

Research on Construction and Application of Cybersecurity Situation Awareness System

Weichao Liang

Jiangmen Public Security Bureau, Jiangmen, Guangdong, 529100, China

Abstract

As an important means of enhancing network security protection capabilities, the network security situation awareness system has been widely applied in public security networks and cloud computing big data environments in recent years. This system helps identify potential threats and risks through real-time monitoring and analysis of network security situations, providing decision-makers with accurate security status feedback. This paper explores the construction methods and application practices of the network security situation awareness system, first analyzing the definition, core components, and technical challenges of network security situation awareness. It then elaborates on key technologies such as data collection, data fusion, and threat modeling, and presents the design principles and key modules of the system architecture. Through application analysis in public security networks and cloud computing big data environments, the paper demonstrates the application value and practical effects of the system. Finally, the paper discusses the optimization paths and future development trends of situation awareness technology, offering new ideas and technical support for network security protection.

Keywords

network security situation awareness; data collection; threat modeling; public security network; cloud computing; system integration

网络安全态势感知体系构建与应用研究

梁伟超

江门市公安局，中国·广东 江门 529100

摘要

网络安全态势感知体系作为提升网络安全防护能力的重要手段，近年来在公安网络和云计算大数据环境得到了广泛应用。该体系通过对网络安全态势的实时监测与分析，帮助识别潜在威胁与风险，并为决策者提供准确的安全状况反馈。本文探讨了网络安全态势感知体系的构建方法与应用实践，首先分析了网络安全态势感知的定义、核心构成及其技术挑战；随后，阐述了数据采集、数据融合与威胁建模等关键技术；并提出了体系架构设计原则与关键模块。通过在公安网络及云计算大数据环境中的应用分析，本文展示了该体系的多重应用价值与实际效果。最终，本文讨论了态势感知技术的优化路径及未来发展趋势，为网络安全防护提供了新的思路和技术支持。

关键词

网络安全态势感知；数据采集；威胁建模；公安网络；云计算；系统集成

1 引言

随着信息化进程的不断推进，网络安全形势愈加严峻，网络攻击手段不断演化，导致网络防御体系面临巨大的挑战。传统的网络安全防护方式难以应对复杂的网络攻击模式，因此，网络安全态势感知技术作为应对这一问题的有效手段应运而生。网络安全态势感知通过实时监测网络环境、分析潜在威胁、评估安全风险，为决策者提供科学依据。其核心在于信息的采集、融合与智能分析，而如何构建一个高效、实时的安全态势感知体系，成为当前研究的重点。随着大数据、云计算和人工智能等技术的迅速发展，网络安全态势感知的技术框架和应用范围也在不断拓展。因此，探索网络安全态势感知体系的构建与应用，

【作者简介】梁伟超（1985–），男，中国广东江门人，本科，工程师，从事计算机信息技术、网络信息技术、网络空间安全研究。

已成为提升网络安全防护能力的关键课题。

2 网络安全态势感知体系构建的理论基础

2.1 网络安全态势感知的定义与重要性

网络安全态势感知是指通过对网络环境中各类信息进行实时采集、分析与处理，全面监控网络安全状况，识别潜在威胁与风险的技术过程。其重要性在于，随着信息化的发展，网络安全问题日益复杂，传统的防护手段已无法应对新型的网络攻击。通过建立态势感知体系，可以在事前、事中与事后对网络安全进行动态监测与评估，及时发现攻击活动与漏洞，提供高效的决策支持。态势感知有助于提升网络防御能力，减少潜在的网络风险，保障数据安全、信息完整性以及业务连续性[1]。

2.2 网络安全态势感知体系的核心构成

网络安全态势感知体系主要由数据采集层、数据处理层与决策支持层构成。数据采集层通过各种传感器与网络监测设备实时获取来自不同设备和系统的数据，包括流量数据、日志数据和安全事件等。数据处理层负责对采集的数据进行清洗、归类与存储，并利用数据分析技术对数据进行深度处理，识别网络中的潜在安全威胁与攻击行为。决策支持层则基于处理后的数据，结合机器学习与人工智能算法，为安全管理人员提供实时警报与决策依据。该体系通过多层次的协同作用，将各个环节紧密结合，确保网络安全态势的全面感知与实时响应。

3 网络安全态势感知体系的构建方法

3.1 数据采集与监测技术

数据采集与监测技术是网络安全态势感知体系的基础，它负责收集来自各个节点、设备及系统的数据。常用的采集方法包括网络流量监测、入侵检测系统（IDS）、安全信息与事件管理系统（SIEM）、以及日志管理工具等。这些技术能够实时捕捉网络中发生的安全事件，监测到系统的运行状态，识别可疑行为与异常流量。通过深度包检测（DPI）技术，可以进一步对网络流量进行分析，识别潜在的恶意行为。此外，为了提高数据采集的广度与精度，公安网络还部署了高频次的传感器与探针，采集各种网络层级的数据。数据的可靠性和准确性对于后续的分析至关重要，因此，采集技术必须具备高效、准确且低延迟的特点，以支持高强度的实时监控需求。随着网络安全形势的复杂化，采集技术还需支持对加密流量、物联网设备以及云环境的适配与监控，以应对新型网络环境的挑战。

3.2 数据融合与智能分析方法

数据融合与智能分析方法通过将来自不同来源的数据进行整合，提升对网络安全态势的全面感知能力。数据融合的核心在于将异构数据源的原始信息进行统一处理，消除信息冗余，提取关键信息。通过多源数据融合，可以准确识别出各类攻击模式与潜在风险。智能分析方法采用机器学习、深度学习等技术，对融合后的数据进行模式识别、异常检测与威胁分析。例如，基于监督学习的分类算法可以通过历史数据训练模型，识别出潜在的攻击类型；基于聚类分析的无监督学习方法可以自动发现新的攻击模式。智能分析方法不仅能够提高对已知攻击的检测精度，还能挖掘出未知的安全威胁，提升预警能力。随着人工智能技术的发展，越来越多的自学习算法被引入到数据融合与分析中，使得网络安全态势感知更加智能化、自动化[2]。

3.3 网络安全威胁建模与预测方法

网络安全威胁建模与预测方法用于识别潜在的安全威胁，并根据现有数据和历史趋势进行攻击预测。这些方法通常依赖于统计分析、机器学习、以及基于图形的建模技术。威胁建模首先通过收集历史安全事件数据，分析攻击行为的模式与特点，构建攻击图与攻击树，从而识别出网络中最脆弱的部分。利用概率模型与贝叶斯网络等方法，可以对攻击路径与攻击成功率进行预测。随着大数据技术的发展，基于大数据分析的威胁预测方法逐渐成为主流，它可以在海量的数据中识别潜在的攻击趋势，并对未来的攻击活动进行预警。此外，机器学习中的回归分析与时间序列预测方法也被应用于网络安全威胁预测，以识别出攻击行为发生的时间和可能性。通过精确的威胁建模与预测，网络安全防护系统能够提前做出响应，最大程度降低网络攻击对公安业务、云计算平台的影响。

4 网络安全态势感知体系的架构设计

4.1 体系架构的设计原则与框架

网络安全态势感知体系的架构设计需要遵循高效性、可扩展性和实时性的原则。高效性要求体系能够在高流量、高并发的环境中迅速处理大量数据，确保对网络事件的及时反应。可扩展性则确保架构能够适应不断变化的公安网络、云计算环境与安全需求，能够灵活扩展以处理新型威胁的出现。实时性是态势感知体系最为关键的要求之一，要求体系能够对网络环境中的动态变化做出即时响应。此外，架构设计还需确保数据的高保真性与一致性，采用多层数据采集与传输方式，确保信息的完整性与精确性。数据采集层负责从网络中各个节点和设备获取原始信息，数据融合与分析层对采集的数据进行清洗、处理与智能分析，最终生成网络安全态势报告，供决策层参考。整个架构需要具备自动化、智能化的特征，通过深度学习与数据挖掘技术，不断优化对未知攻击的检测能力[3]。

4.2 关键模块与功能设计

网络安全态势感知体系的关键模块包括数据采集模块、数据处理模块、威胁分析模块和决策支持模块。数据采集模块负责从不同数据源中获取实时网络流量、日志信息、安全事件等数据，通过分布式传感器与探针进行监控。数据处理模块对原始数据进行清洗、格式化与存储，确保数据的高效存取与高质量分析。威胁分析模块则基于多种技术，如机器学习、深度学习和模式识别，对数据进行深度分析，识别潜在的攻击模式。该模块不仅能够分析已知的攻击类型，还能通过自学习机制发现新的安全威胁。决策支持模块负责将分析结果转化为可操作的安全事

件报告，向管理人员提供实时警告与应对策略。该模块结合人工智能技术，能够实现智能推荐与自动化响应，使得公安网络、云计算环境安全管理更加高效。每个模块的数据流动需要高度协同，通过数据总线技术确保数据的实时传递与处理，减少延迟，提高响应速度。

4.3 技术架构与系统集成方案

网络安全态势感知体系的技术架构主要基于分布式计算与云计算平台，采用微服务架构实现各个功能模块的独立性与高效协作。数据采集层利用物联网技术与边缘计算节点对公安网络、云计算节点中的各个环节进行实时监测，采集的数据通过安全通道传输到数据处理层。数据处理层采用大数据处理技术，如Hadoop与Spark进行海量数据的并行计算与存储，确保系统的扩展性与高效性。在数据分析与决策支持层，利用机器学习与人工智能算法进行数据挖掘与安全事件的预测。系统集成方案则通过API与标准化协议将不同设备与系统连接，确保各类数据源的兼容性与信息的无缝对接。为实现系统的高可用性与灾备能力，系统架构还需要结合云平台的弹性计算与容灾备份机制，确保在发生系统故障时能够自动切换与恢复。通过这样的技术架构与系统集成方案，网络安全态势感知体系能够实现对公安网络、云计算大数据复杂环境的高效感知与管理，提供强有力的安全保障。

5 网络安全态势感知体系的应用分析

5.1 网络安全态势感知在网络流量监测中的应用

网络流量监测是网络安全态势感知体系中的基础应用。通过实时监控公安网络、云计算平台流量，系统能够及时发现异常流量、突发流量和恶意攻击行为。流量监测技术依赖深度包检测（DPI）与流量分析技术，对进出网络的数据包进行深度分析与分类。基于这些技术，能够快速识别并标记出异常流量，如DDoS攻击、恶意扫描等。通过流量监测模块，网络安全体系可以实现对公安网络、云计算环境活动的全面可视化，使管理员能够即时了解网络状况，并进行早期威胁检测。数据采集层收集网络中的每个数据包，并通过流量分析引擎对数据包进行分析与筛选，提取有用的安全信息。在此基础上，系统可通过机器学习算法对网络流量模式进行建模，从而提高对未知攻击类型的检测能力，确保在公安网络、云计算环境中潜在威胁发生时做出即时响应[4]。

5.2 网络安全态势感知在入侵检测与防御中的应用

入侵检测与防御是网络安全态势感知体系的重要应用之一。通过入侵检测系统（IDS）与防火墙等技术的结合，态势感知体系能够实时监测到公安网络、云计算环境中的非法入侵行为，并立即采取相应的防御措施。基于签名匹配与异常行为分析，入侵检测系统能够识别常见的攻击手段，如SQL注入、缓冲区溢出攻击等。同时，随着深度学习技术的发展，入侵检测系统逐渐引入了智能化分析，利用算法模型对行为模式进行识别，增强了对未知攻击的检测能力。在数据采集过程中，系统收集公安网络、云计算环境流量、日志与安全事件等信息，通过数据融合技术对这些数据进行深度分析，评估潜在的攻击风险。当检测到攻击行为时，系统能够自动启动防御机制，如阻断攻击流量、封堵恶意IP等，确保公安网络、云计算环境的安全性与稳定性。

5.3 网络安全态势感知在风险评估与预警中的应用

公安系统中的网络安全态势感知体系，通过持续监控公安网络、云计算大数据环境运行状态与安全数据，实现对关键信息基础设施、警务平台及数据资源的全面风险评估与预警。系统能够汇总来自不同节点、终端和业务系统的安全事件数据，评估公安网络面临的潜在威胁，并给出风险评分。借助数据挖掘与机器学习算法，不仅可以识别当前存在的安全风险，还能预测未来可能的攻击趋势与系统漏洞，提升对网络攻击行为的预判能力。

通过构建针对公安业务、云计算场景的攻击模型与风险评估框架，态势感知系统可实时生成安全分析报告，为公安信息中心、指挥调度部门等提供及时、准确的预警信息。分析结果以可视化方式呈现，便于安全管理人员快速掌握风险态势、定位薄弱环节，并采取针对性防护措施。此外，系统可与国家网络安全情报中心、行业威胁情报平台等外部数据源对接，集成多方安全情报，增强对新型网络攻击、APT（高级持续性威胁）等复杂威胁的响应能力，保障公安信息系统、云计算大数据平台的持续安全运行。

6 结语

通过对网络安全态势感知体系的构建与应用分析，可以看出该体系在提升公安网络、云计算环境安全防护能力方面具有重要意义。随着网络环境日益复杂，传统的防护手段已难以应对新型的安全威胁，而态势感知体系通过实时监测、智能分析和快速响应，能够有效识别潜在风险并提供及时的防御措施。数据采集、融合分析和威胁预测技术的不断发展，使得该体系不仅能够对已知攻击进行准确识别，也能对未知威胁做出有效预警。未来，随着技术的持续进步，网络安全态势感知体系将不断优化，在保障公安网络、云计算平台安全、提高应急响应能力以及加强数据保护等方面发挥更加重要的作用。

参考文献

[1] 吴存寿,程瑞东,任重,张琦钢,叶培彬.基于聚类算法的网络安全态势感知平台系统设计研究[J].中国新技术新产品,2026,(05):134-136.

[2] 刘玥,叶飞.智能运维工具在公安网络故障排除中的应用[J].中国安防,2026,(03):8-10.

[3] 刘峰,刘延峰,孙文豪.大模型在公安网络安全领域深度应用的路径探索[J].网络安全和信息化,2026,(01):26-28.

[4] 张萌。多源数据融合的网络安全态势感知方法研究 [J]. 网络安全技术与应用，2025 (02):45-47.

[5] 赖雄辉.公安系统网络安全防护能力提升思路与建议[J].网络安全技术与应用,2023,(09):130-132.