构建智能预测分析系统加强网络安全工程的安全防御能力

牟家刘

中国电子技术标准化研究院，北京市东城区，100000；

摘要：随着互联网和大数据技术的发展，网络安全问题呈现出新的特点和趋势。本文从大数据技术角度出发，提出了一种基于智能预测分析的网络安全工程安全防御系统架构，并通过多个应用案例说明了其在网络安全中的具体作用。通过分析目前网络安全工程面临的主要挑战，探讨了智能预测分析在网络安全中的应用场景，提出了构建智能预测分析系统加强网络安全工程的安全防御能力。最后，基于多个应用案例和实验分析了该系统在提高网络安全工程防御能力方面的作用效果。本文研究成果将对大数据技术在网络安全工程中的应用提供一定借鉴和参考。

关键词：大数据技术；网络安全工程；智能预测分析；安全防御

DOI：10.69979/3060-8767.25.03.077

引言

随着互联网技术和大数据技术的快速发展，网络安全问题呈现出新的特点和趋势，网络安全问题已经成为当今世界各国共同面临的严峻挑战之一。近年来，我国在网络安全领域取得了长足进步，但仍然存在着诸多安全问题，需要不断提升网络安全防护水平。基于此背景，本文在对大数据技术进行了分析和研究后，从大数据技术角度出发，提出了一种基于智能预测分析的网络安全工程安全防御系统架构，并通过多个应用案例说明了其在网络安全中的具体作用。最后，本文从系统设计、关键技术和应用效果三个方面对该系统进行了案例分析和实验研究。

1 网络安全工程概述

1.1 网络安全工程概念及重要性

网络安全工程（Cybersecurity Engineering，CSE）是将网络安全作为一个整体来考虑，同时对整个系统进行安全评估、设计、部署、运营和维护。在网络安全工程中，对整个网络进行整体的安全评估和设计是至关重要的。通过设计网络的安全防御体系来提高整体系统的安全性。网络安全工程的主要任务是制定一个整体的安全战略和计划，包括明确攻击目标、信息获取、保护关键基础设施，同时还要确定如何通过一系列措施来保护关键基础设施[1]。网络安全工程在整个信息化时代中发挥着关键作用，是维护国家安全和发展利益的重要保障。

1.2 网络安全工程的发展现状

随着计算机的普及，网络已成为人们生活中不可缺少的一部分，对人们的生活和工作也产生了很大的影响。但与此同时，网络安全问题也日益凸显出来，各种攻击手段层出不穷，网络安全已经成为一个严峻的社会问题。目前我国网络安全工程正处于发展初期，还不能很好地适应日益发展的网络空间。由于我国计算机和通信技术水平相对落后，在面对各种安全威胁时往往不能有效应对，在一定程度上阻碍了我国互联网安全工程的发展。因此，应加快我国计算机和通信技术水平的发展和提升，使其能够更好地满足网络安全工程建设的需求。

1.3 网络安全工程面临的挑战

随着全球数字经济的快速发展，网络安全问题也日益凸显，网络攻击手段更加多样、攻击方式更加复杂、攻击成本越来越低、攻击效果越来越精准，网络安全防御技术面临新的挑战。网络安全工程的主要目标是预防和控制网络风险，以保护网络和系统的安全。然而，许多人并没有意识到在实际情况下如何做出明智的决策。随着互联网技术的快速发展，网络攻击的成本也越来越低，其效果越来越精准，这给网络安全带来了更大的挑战。目前，没有一种通用的方法可以在所有情况下都有效地保护网络系统。因此，建立一套通用的、可扩展的方法来评估和预测网络风险是非常重要的。

2 大数据技术在网络安全中的应用

2.1 大数据技术概述

大数据技术是指利用现代信息技术对海量数据进行收集、存储、管理、处理和分析的一种新型技术。大数据具有数据量大、种类多、来源分散等特点，目前已在信息获取与信息处理等方面得到了广泛应用。随着科学技术的发展，大数据技术在企业管理中也得到了越来越多的应用，其优势包括：帮助企业挖掘数据信息的价值，实现对数据的价值分析；优化企业生产流程，提高生产效率；优化企业市场运营模式，增强企业市场竞争力等。通过使用大数据技术可以帮助企业更加科学地制

定营销策略，更好地把握市场动态和竞争趋势，实现产品的更新换代。

2.2 大数据技术在网络安全中的优势

在网络安全中应用大数据技术，一方面，可以通过大数据技术对网络中的各类数据信息进行收集、整理和分析，从而掌握网络安全状况，以此为依据，更好地防范和应对网络安全威胁。另一方面，大数据技术具有一定的开放性、多样性等特点，在收集、处理和分析网络安全信息方面具有一定的优势。而且，大数据技术还具有以下几个方面的优势：首先，大数据技术可以为网络安全防御提供全方位、多角度的信息，对网络安全防御工作起到重要的支撑作用；其次，大数据技术可以提高对网络安全威胁的预测能力和防范能力；最后，大数据技术还能为网络安全防御工作提供准确、可靠的分析结果。

2.3 大数据技术在网络安全中的应用案例

网络安全中的应用案例多种多样，网络安全中的数据采集过程包括：网络设备和其他设备中的数据采集；用户通过客户端对互联网上的信息进行收集，并将这些信息输入到服务器中；服务器会根据用户的输入内容，进行数据处理，并将处理结果反馈给用户[2]。大数据技术在网络安全中的应用主要体现在：通过大数据技术，可以收集到大量的数据，而这些数据都是具有价值的，可以为网络安全提供帮助。而大数据技术在网络安全中应用的一个重要方面就是可以对收集到的数据进行处理，这样可以及时发现系统中存在的安全隐患，并将这些隐患及时地解决掉。

3 智能预测分析在网络安全中的作用

3.1 智能预测分析概述

在网络安全的各个领域，智能预测分析系统的关键能力是能够更好地处理大数据，并快速、准确地对新的、未知的威胁进行预测和分析。这一点是传统防御手段所无法达到的。随着网络安全威胁的日益复杂，以及网络安全防御系统和防御体系的日益完善，传统的手工分析方法已不能满足需要。因此，智能预测分析技术被提出来解决这一问题。其主要功能是将实际威胁数据与预测模型进行结合，然后根据所选模型对未来数据进行预测，从而帮助网络安全人员做出正确的决策。智能预测分析技术还可以为网络安全防御系统提供更高级别的威胁预警，以实现更准确的网络安全防御。

3.2 智能预测分析在网络安全中的优势

（1）提高检测和响应速度。在网络安全的早期阶段，由于攻击行为的随机性和不可预测性，很难确定网络安全事件的发生时间。随着攻击行为的演变，攻击者对网络安全事件的响应时间将越来越短，而智能预测分析可以通过收集到的大量数据和攻击过程中使用的特征信息来预测未来攻击行为[3]；（2）提高对威胁行为的识别能力。智能预测分析可以根据收集到的数据和专家经验来识别出潜在的攻击行为，这不仅可以降低误报率和漏报率，还可以为网络安全防御提供决策依据；（3）提高防御效果。智能预测分析可以使网络安全防御系统变得更加灵敏，并及时发现新威胁行为。

3.3 智能预测分析在网络安全中的应用场景

从当前网络安全的现状来看，智能预测分析在网络安全中的应用场景主要有以下三种：一是当发现漏洞后，及时通知用户采取相应措施，避免用户遭受损失；二是当发现漏洞后，通过分析漏洞产生的原因，帮助用户进行改进，避免再次发生类似事件；三是当发现漏洞后，通过智能预测分析系统对相关攻击进行预测，指导用户采取防御措施。智能预测分析在网络安全中的应用场景，一方面可以帮助用户及时发现网络安全事件并进行预防、解决；另一方面可以根据用户的反馈数据不断优化安全防御体系的策略，提升整个网络的安全性。

4 构建智能预测分析系统加强网络安全工程安全防御能力

4.1 系统架构设计

本文提出的智能预测分析系统基于传统网络安全中的态势感知技术，结合机器学习算法，融合人工智能、大数据等新兴技术，依托成熟的数据挖掘、机器学习等技术，实现对网络安全中攻击流量、威胁行为、资产漏洞等信息的预测分析，形成智能态势感知和预测分析能力。系统架构设计主要分为数据层、平台层和应用层三个层面。其中数据层主要实现对网络安全数据的采集和处理，并提供统一的接口；平台层是整个系统的核心，对采集到的数据进行处理和分析，并提供统一的接口；应用层则是将处理后的数据分析结果呈现给用户。

4.2 数据收集与处理模块

在数据收集与处理模块中，数据的来源主要是网络安全工程各个环节产生的数据。这部分的数据来源包括：各类网络安全事件产生的日志，包括入侵检测系统（IDS）、防火墙、入侵防御系统（IPS）、 Web 应用防火墙、网络防病毒系统（SVAC）等，以及各类安全服务提供商（ISP）和安全服务提供商（SP）提供的各类安全服务和产品[4]。这部分的数据收集与处理模块主要是对收集到的各类安全事件进行分析和处理，例如对网络攻击事件进行分析，将攻击事件与安全事件关联，对网络安全事件进行统计分析等，从而达到对网络安全事件进行预

测和分析的目的。

4.3 预测分析模块

在网络安全工程中，其所产生的大量数据不仅对系统本身有价值，而且还能为系统运行提供决策支持，进而影响到系统的安全性。在传统的网络安全防御体系中，通过检测网络流量和网络安全事件等数据信息，能有效发现异常行为和安全事件。但这些数据信息一般都是由人工手动提取的，存在一定的滞后性。而智能预测分析模块能够实现对大量历史数据的实时分析和动态处理，能在网络安全防御体系中发挥重要作用。例如，可以将收集到的大量网络流量数据信息、相关设备数据信息、安全事件等进行处理分析，并将处理分析结果以可视化界面展示出来。

4.4 安全防御策略

智能预测分析系统能够帮助用户在短时间内快速地了解网络安全工程的潜在威胁，进而采取相应的防御策略，保证网络安全工程的安全。因此，用户需要根据预测分析系统提供的信息，制定合适的网络安全工程防御策略。例如，某单位在网络安全工程中部署了智能预测分析系统，并且根据预测分析系统提供的信息制定了详细的防御策略。该单位将智能预测分析系统应用于网络安全工程中，结果发现该单位的网络安全工程受到了攻击。在随后的调查中发现该单位已经采取了防御措施，因此该单位没有受到攻击。由此可见，智能预测分析系统能够有效帮助用户制定合理的防御策略。

4.5 系统实施与评估

智能预测分析系统在网络安全工程中的应用，应由国家政策引导，结合我国实际情况，从我国实际出发，以《中华人民共和国网络安全法》为基础，结合当前人工智能、大数据、物联网等技术发展情况，在广泛调研、深入分析的基础上进行建设。在系统实施过程中，要紧密结合国家相关政策、法律法规的要求，确保系统建设符合国家相关政策和法律法规。在智能预测分析系统运行过程中，要根据实际情况进行调整、升级和改进。同时，为了确保系统的安全稳定运行，应做好智能预测分析系统的安全评估工作。在实施过程中要定期对系统进行评估和验证。

5 案例分析与实验

5.1 设计案例研究

案例研究对象是某地区公安部门的网络安全工程，其具有海量的数据，在人工智能预测分析系统中采用机器学习算法来处理这些数据，然后将处理后的数据运用于网络安全工程安全防御能力的提升。具体来看，该案例研究对象的网络安全工程主要包括以下几个方面：（1）数据收集：对网络安全工程中的安全数据进行收集、整理和分类；（2）机器学习算法：在数据收集与整理完毕后，采用基于机器学习算法的网络安全工程预测分析系统对网络安全工程中的数据进行分析；（3）系统建立：根据对网络安全工程中的数据分析结果，对网络安全工程中存在的安全风险进行识别并给出相应的防御建议。

5.2 实验设计与数据分析

实验平台搭建了基于开源框架的大数据智能预测分析系统。实验平台包括了数据采集、数据存储、数据分析、系统管理等多个模块。在此基础上，对该智能预测分析系统的整体性能进行了测试，具体包括：训练阶段（训练集与测试集）、预测阶段（预测集与真实数据）、监控阶段（监控节点与预测节点）等。该智能预测分析系统在部署使用时，可根据实际业务需求对其进行二次开发，并在业务部门和安全部门之间进行数据共享。实验结果表明，该智能预测分析系统具有良好的性能，能够快速高效地实现对网络安全事件的预测，为网络安全防御提供技术支撑。

6 结语

随着大数据技术和物联网、人工智能技术的发展，网络安全工程面临着新的挑战，需要不断提高网络安全工程的防御能力。本文提出了一种基于智能预测分析的网络安全工程安全防御系统架构，该系统能够在保护网络资源和数据的同时，利用大数据技术对网络安全态势进行智能预测分析，并对其进行全面评估，从而不断提高网络安全工程的防御能力。本文构建了智能预测分析系统，并通过案例分析和实验研究对该系统进行了验证。结果表明，该系统能够在短时间内对网络安全态势进行准确判断，从而实现对潜在攻击行为的实时监测和预警，并自动生成相应的防御措施。

参考文献

[1]曾鹏.基于大数据分析的智能采购需求预测系统研究与实现[J].软件,2025,46(05):145-147.
[2]张忠江,王志学.基于大数据分析的公路交通流量智能预测系统设计[J].交通科技与管理,2025,6(08):22-24.
[3]孙振超,王路,孙国青.人工智能在电力通信系统故障诊断与预测分析[J].家电维修,2025,(01):68-70.
[4]黄鑫,陈美龙,陈芬,等.基于智能网关的低压光伏出力控制系统分析[J].电子技术,2024,53(12):152-153.