Computer Science and Application 计算机科学与应用, 2025, 15(3), 119-128
Published Online March 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.153064

Hans汉斯

基于大数据分析的网络攻击主动防御系统

刘子豪，康晓凤，何培延，王　伟，沈楷博，赵浩东

徐州工程学院信息工程学院(大数据学院)，江苏　徐州

收稿日期：2025年2月14日；录用日期：2025年3月13日；发布日期：2025年3月20日

摘　要

随着网络攻击手段的多样化和攻击规模的持续扩大，如何实现主动防御与实时威胁分析成为网络安全领域的核心挑战。本文提出了一种基于大数据分析的网络攻击主动防御系统，该系统采用Streamlit框架进行轻量化部署，结合MySQL数据库进行攻击数据存储，并利用支持向量机回归(SVR)模型预测潜在攻击目标。系统包含蜜罐监控、攻击数据实时分析、IP及端口词云可视化、攻击预测及端口智能分类等核心模块，能够高效捕获、分析并预测攻击行为。通过蜜罐技术，系统可实时检测远程代码执行(RCE)、SQL注入、XSS攻击等常见网络攻击，并结合机器学习模型动态评估未来攻击趋势。实验结果表明，该系统在大规模网络环境下具备高效的攻击检测能力，并能够通过可视化手段提升安全态势感知能力。相较于传统防御机制，本系统不仅可以在攻击发生时进行响应，还可提前预测攻击风险，为主动防御提供智能化支持，适用于高复杂度网络环境中的安全防护。

关键词

主动防御，支持向量机回归，蜜罐，大数据分析

Big Data-Based Active Defense System Against Cyber Attacks

Zihao Liu, Xiaofeng Kang, Peiyan He, Wei Wang, Kaibo Shen, Haodong Zhao

College of Information Engineering (Big Data College), Xuzhou University of Technology, Xuzhou Jiangsu

Received: Feb. 14th, 2025; accepted: Mar. 13th, 2025; published: Mar. 20th, 2025

Abstract

With the increasing diversity of cyberattack methods and the continuous expansion of attack scale, achieving proactive defense and real-time threat analysis has become a core challenge in the field of cybersecurity. This paper proposes a big data-driven active cyber defense system that utilizes the Streamlit framework for lightweight deployment, MySQL database for attack data storage, and

文章引用: 刘子豪, 康晓凤, 何培延, 王伟, 沈楷博, 赵浩东. 基于大数据分析的网络攻击主动防御系统[J]. 计算机科学与应用, 2025, 15(3): 119-128. DOI: 10.12677/csa.2025.153064

Support Vector Regression (SVR) to predict potential attack targets. The system integrates key modules such as honeypot monitoring, real-time attack data analysis, IP and port word cloud visualization, attack prediction, and intelligent port classification, enabling efficient attack detection, analysis, and prediction. Leveraging honeypot technology, the system can detect real-time cyber threats, including Remote Code Execution (RCE), SQL injection, and XSS attacks, while employing machine learning models to dynamically assess future attack trends. Experimental results demonstrate that the system effectively detects attacks in large-scale network environments and enhances security situational awareness through visualization techniques. Compared to traditional defense mechanisms, this system not only responds to ongoing attacks but also anticipates potential threats, providing intelligent support for proactive defense and making it well-suited for cybersecurity protection in highly complex network environments.

Keywords

Active Defense, Support Vector Regression (SVR), Honeypot, Big Data Analysis

1. 引言

近年来，现有的主动防御系统在实际应用中仍然存在诸多问题，主要包括攻击检测的实时性不足、数据分析能力有限、攻击预测能力薄弱以及可视化水平较低，难以满足现代复杂网络环境下的安全需求。

针对这些问题，本文提出了一种基于大数据分析的网络攻击主动防御系统，通过集成蜜罐技术、机器学习模型和可视化分析工具，实现攻击行为的主动捕获、智能分析及未来攻击趋势预测。系统采用轻量化的前端框架 Streamlit，结合高效的数据存储与管理方案 MySQL 数据库，支持多维度攻击数据的展示和实时日志存储，确保大规模网络环境下的数据处理效率。系统通过蜜罐模块监测恶意流量，识别包括远程代码执行(RCE)、SQL 注入、XSS 攻击等常见的网络攻击行为，并结合支持向量回归(SVR)进行攻击趋势预测，为安全管理人员提供数据驱动的决策支持。

此外，为了提升网络安全防御的可视化分析能力，系统提供 IP 和端口词云图、地理位置分析、攻击趋势图等可视化功能，使安全管理人员能够直观了解当前的攻击态势，快速定位攻击源，并采取相应防御措施。相比传统的主动防御系统，本文提出的方案不仅能够在攻击发生时进行检测和响应，还能够提前预测潜在威胁，提高网络安全的主动防御能力，适用于高复杂度网络环境下的安全防护。

2. 技术特点

2.1. 蜜罐监控与攻击捕获

2.1.1. 蜜罐技术概述

蜜罐(Honeypot)是一种安全机制，最初在 1989 年出版的《The Cuckoo’s Egg》小说[1]中得以引入，它通过模拟真实系统环境吸引攻击者，从而诱导其发起攻击，并记录攻击过程，以便进一步分析。蜜罐的核心目标是欺骗攻击者，使其暴露攻击方法和工具，同时避免对真实系统造成破坏。该技术在网络安全研究、恶意软件分析、入侵检测系统优化等领域具有重要作用。根据交互程度，蜜罐可分为低交互蜜罐、高交互蜜罐和分布式蜜罐，其中低交互蜜罐主要通过模拟简单的登录界面或端口相应记录攻击者的基本信息，高交互蜜罐可提供更真实的服务器环境，深入捕获攻击者行为，但维护成本较高[2]，而分布式蜜

罐主要适用于复杂的系统防御环境，具备大批量感知攻击态势的能力，但部署和管理复杂。现有研究表明，结合机器学习技术的蜜罐系统能够提升攻击检测能力，但仍面临绕过检测、数据存储压力大、缺乏预测能力等挑战[3]。在本系统中，蜜罐技术用于捕获主动攻击流量，包括但不限于远程代码执行 RCE、SQL 注入、XSS 跨站脚本攻击、端口扫描和 DDoS 攻击等常见的攻击方式。所有捕获的数据都会被详细记录，并存储到日志文件中，供后续的攻击分析和安全策略调整使用。

2.1.2. 蜜罐系统的工作流程

本系统的蜜罐监控与攻击捕获功能主要包括流量捕获、攻击分析、日志存储三个核心步骤。

1) 流量捕获

通过网络监听技术，系统能够实时监测流经蜜罐的网络流量，并解析数据包，提取攻击相关的信息，包括源 IP 地址、目标端口、攻击时间、攻击类型等。在捕获流量的过程中，蜜罐会模拟真实服务器的响应行为，以保持欺骗性，使攻击者误以为其正在攻击一个真实的系统，而不是一个安全研究环境。

2) 攻击分析

通过攻击行为特征匹配，系统能够自动识别并分类不同类型的攻击，例如 SQL 注入、远程代码执行(RCE)、暴力破解等[4]。

使用模式匹配技术对请求进行分析，判断攻击者是否尝试利用某些已知漏洞或攻击方式。利用日志分析和可视化工具，系统可以将捕获的攻击数据进行处理，形成可视化报告，以便管理员快速掌握网络攻击态势。

3) 日志存储与管理

所有捕获的攻击行为都会被存储到 traffic_monitor.log 日志文件中，并定期存入 MySQL 数据库，以便进行后续分析和溯源[5]。管理员可以使用系统提供的查询工具，查看特定时间段内的攻击记录，并生成报告，为网络安全防御提供决策依据。

2.2. 支持向量机回归特点分析与算法

1) 高效的回归性能

SVR 通过构建一个超平面(回归函数)，使得该平面尽可能与数据点之间的偏差最小化[6]。与传统回归算法相比，SVR 具有更强的鲁棒性，即使面对噪声数据或离群点时，仍能保持较高的准确性。SVR 在回归问题中通过最大化容许误差范围来确保在给定误差范围内找到最优解。

回归模型的目标是最小化以下目标函数：

$$\min_{w,b,\epsilon} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}\epsilon_i \quad \text{(公式 1)}$$

其中，w 是超平面参数，C 是正则化参数，ϵ_i 是容许误差，n 是样本数量。

2) 非线性回归能力

SVR 可以通过核技巧(Kernel Trick)来处理非线性回归问题。通过将输入数据映射到更高维的特征空间，SVR 可以在高维空间中找到最优的回归超平面，处理线性不可分的情况。常用的核函数包括径向基核(RBF)、多项式核和线性核。核函数的形式为：

$$K(x,y) = \phi(x)\cdot\phi(y) \quad \text{(公式 2)}$$

其中，$\phi(x)$ 和 $\phi(y)$ 是映射到高维空间的特征函数，$K(x,y)$ 是输入数据点 x 和 y 在高维空间中的内积。

3) 良好的泛化能力

SVR 的目标不仅是最小化训练数据的误差，还要最大化间隔，即使模型对未知数据有较好的泛化能

力。在训练过程中，SVR 通过调节正则化参数 CCC 来平衡训练误差和模型的复杂度，从而避免过拟合问题。合理的 CCC 值可以帮助模型在训练数据和测试数据之间取得平衡，确保模型在未见数据上的表现良好。

SVR 的最优回归函数可以通过以下公式表示：

$$f(x)=w\cdot x+b \tag{公式 3}$$

在高维特征空间中，回归函数的目标是最小化如下损失函数：

$$L(y,f(x))=\sum_{i=1}^{n}\max\left(0,\left|y_i-f(x_i)\right|-\epsilon\right) \tag{公式 4}$$

其中，y_i 是真实标签，$f(x_i)$ 是预测值，ϵ 是允许的误差范围。

4) 参数调优与优化

SVR 的表现高度依赖于超参数的选择，尤其是正则化参数 C、容许误差 ϵ 和核函数。通过对这些参数的调优，可以显著提升预测的精度和鲁棒性。例如，增加 C 值会使模型更加关注减少训练误差，但可能导致过拟合；而调整 ϵ 则能影响模型对误差的容忍度。通过交叉验证(Cross-validation)，可以自动选择最佳的参数组合。

2.3. 攻击数据分析与可视化

1) 攻击数据的多维度分析

时间序列分析：统计每日、每小时或每分钟的攻击数量，发现攻击的高峰时段和周期性模式。攻击 IP 分析：识别最常见的攻击源 IP，并追踪其历史攻击行为，分析其攻击频率和目标。端口和协议分析：统计攻击者针对的端口号及使用的网络协议(如 TCP、UDP、HTTP)，帮助安全人员优化防火墙策略。攻击类型分析：分类统计不同攻击手段的占比，如 SQL 注入、远程代码执行 RCE、暴力破解、DDoS 攻击等，便于管理员了解当前主要的安全威胁。

2) 可视化技术

攻击趋势图：通过折线图、柱状图展示攻击次数随时间的变化，帮助管理员掌握攻击波动情况[7]。攻击源地理位置地图：基于 IP 地理信息库，绘制全球攻击源分布地图，标明攻击者的来源地区。IP 及端口词云图：利用词云图展示被攻击最频繁的 IP 和端口，直观呈现攻击热点。攻击排行榜：列出攻击次数最多的 IP、端口和攻击类型。

3. 系统设计与实现

本系统主要由蜜罐监控、攻击数据分析、攻击预测及数据可视化展示四大部分组成，其中蜜罐监控与攻击预测是其核心功能。蜜罐监控部分基于 Python 和 Streamlit 框架开发，实现对网络流量的实时捕获和日志记录，并自动分析攻击流量。攻击数据分析模块提供一周内的攻击次数、攻击 IP 及地理位置等信息，并以词云、折线图、地图等可视化形式展示攻击模式。攻击预测模块采用支持向量回归(SVR)模型，对历史攻击数据进行学习，预测未来可能的攻击趋势，提高系统的主动防御能力[8]。系统支持蜜罐日志导入 MySQL 数据库，实现高效的数据管理和查询。

3.1. 蜜罐监控模块

蜜罐监控模块基于 TCP/IP 三次握手机制，用于模拟服务器环境，诱导并捕获恶意流量，实现攻击行为的实时监测与记录。系统通过监听指定端口，分析进入的网络数据包，判断其是否属于攻击流量，并将相关信息存入日志。攻击者访问蜜罐时，系统会模拟服务器的 TCP SYN-ACK 响应，与其建立连接，

伪装成正常的服务端，从而诱导攻击者进一步发送恶意请求。本模块支持多种协议如 TCP、UDP、HTTP、HTTPS 等，通过识别所带的负载 Payload 匹配模式，能够识别远程代码执行 RCE、SQL 注入、暴力破解、端口扫描等常见攻击。

为了提高攻击分析能力，系统集成数据包解析与特征匹配算法，通过正则匹配识别已知攻击模式，并记录攻击者的 IP 地址、端口、请求内容等信息。对于 MySQL 认证欺骗，蜜罐能够模拟服务器返回认证包，引导攻击者输入用户名和密码，以捕获更多攻击细节。所有数据将存入 traffic_monitor.log，如图 1 所示，并支持定期导入 MySQL 数据库，方便管理员进行历史查询与攻击溯源。系统还提供蜜罐状态管理功能，支持手动启动/终止蜜罐，并在蜜罐异常终止时自动提示警告。该模块通过实时流量捕获、欺骗式交互与日志分析，有效提升了网络攻击的检测能力，为安全管理人员提供可靠的数据支持。

```
  Source IP: 192.168.2.118
  Destination IP: 117.30.49.148
  Protocol: TCP
  Payload (Base64): XNqv5bw4VY3zwiA2auM1jjqWFM6oPYWYK9yqkm08N8RM0xN577h5a0wHSbG2ieOJxcZY+nvZJwCw9vPFcAqn+xPc2bYOj78HGSLK8KgKiyXEN8I1H
  Full Packet: Ether / IP / TCP 192.168.2.118:49680 > 117.30.49.148:5040 A / Raw
2025-01-15 16:52:35,643 WARNING: ALERT: RCE Attack detected: XNqv5bw4VY3zwiA2auM1jjqWFM6oPYWYK9yqkm08N8RM0xN577h5a0wHSbG2ieOJxcZY+nvZJwCw
2025-01-15 16:52:35,644 INFO: Packet captured: Ether / IP / TCP 117.30.49.148:5040 > 192.168.2.118:49680 PA / Raw
2025-01-15 16:52:35,644 WARNING: RCE Attack detected:
  Source IP: 117.30.49.148
  Destination IP: 192.168.2.118
  Protocol: TCP
  Payload (Base64): AAAAYAVxYAyMElR4tOzIxXN7xE0THCTJxkvIfwYEm60Fo36ek/LReNk2Qq+w5Fg9PaWOPQoIEiclo2cPG/x5y+CKcRC/sHOZGgdBz9XOOxwpgJW7zj5P
  Full Packet: Ether / IP / TCP 117.30.49.148:5040 > 192.168.2.118:49680 PA / Raw
2025-01-15 16:52:35,644 WARNING: ALERT: RCE Attack detected: AAAAYAVxYAyMElR4tOzIxXN7xE0THCTJxkvIfwYEm60Fo36ek/LReNk2Qq+w5Fg9PaWOPQoIEiclo2cPG
2025-01-15 16:52:35,644 INFO: Packet captured: Ether / IP / TCP 117.30.49.148:5040 > 192.168.2.118:49680 PA / Raw
2025-01-15 16:52:35,644 WARNING: RCE Attack detected:
  Source IP: 117.30.49.148
  Destination IP: 192.168.2.118
  Protocol: TCP
  Payload (Base64): AAAAYLkXxzDgSt9QBUKjj3BYyB/v5LZCDKwrxqmYBUnxJqWdjvLYAx8Re9GqvcD5HIqnfiX0qUJxVmsrxM1foeDZC36tnASFcjiNfJGt/0XpTKIGx7kbJUjaC
  Full Packet: Ether / IP / TCP 117.30.49.148:5040 > 192.168.2.118:49680 PA / Raw
2025-01-15 16:52:35,644 WARNING: ALERT: RCE Attack detected: AAAAYLkXxzDgSt9QBUKjj3BYyB/v5LZCDKwrxqmYBUnxJqWdjvLYAx8Re9GqvcD5HIqnfiX0qUJxVmsrxM
2025-01-15 16:52:35,644 INFO: Packet captured: Ether / IP / TCP 117.30.49.148:5040 > 192.168.2.118:49680 A
2025-01-15 16:52:35,644 INFO: Packet captured: Ether / IP / TCP 117.30.49.148:5040 > 192.168.2.118:49680 A
2025-01-15 16:52:35,645 INFO: Packet captured: Ether / IP / TCP 117.30.49.148:5040 > 192.168.2.118:49680 A
```

Figure 1. traffic_monitor.log file information
图 1. traffic_monitor.log 文件信息

3.2. 攻击数据分析

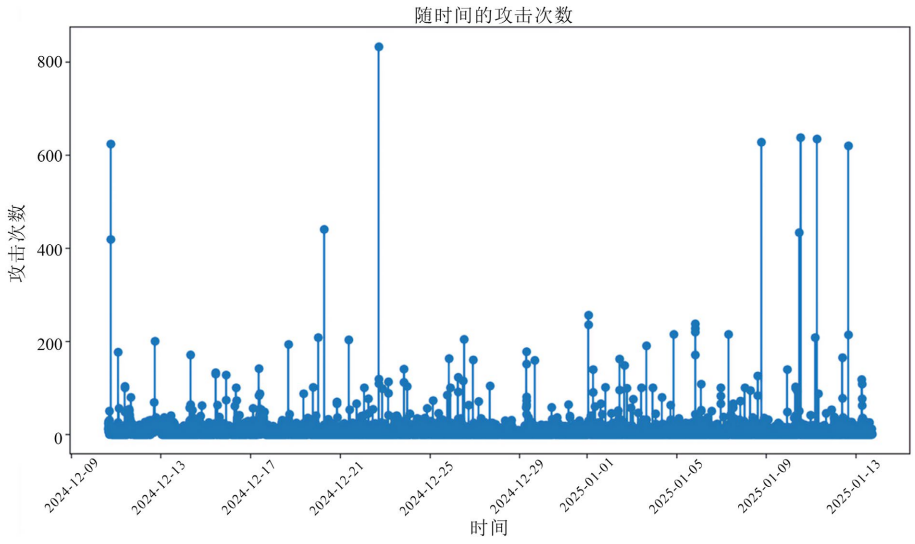

Figure 2. Attack count analysis over time
图 2. 攻击次数随时间分析

Figure 3. Geolocation trace and attack method tracking
图 3. 地理位置溯源及攻击方式追踪

攻击数据分析模块通过对蜜罐捕获的攻击流量进行深入解析，帮助管理员识别攻击模式、溯源攻击来源，并评估潜在的安全威胁。本模块整合攻击趋势分析、攻击类型分类、攻击来源追踪等功能，提供全面的数据支持，便于制定针对性的安全防御策略。系统支持一周内的攻击次数统计，并采用折线图、柱状图展示攻击行为的时序变化，如图 2 所示，帮助管理员掌握攻击高峰期，分析攻击活动的周期性。此外，系统基于 IP 归属地查询，绘制全球攻击源分布地图，直观展示攻击者的地理分布情况，如图 3 所示，有助于识别特定地区的恶意流量，为防御措施提供数据支持。

Result Grid | Filter Rows: | Edit: | Export/Import: | Wrap Cell Content: | Fetch rows:

id	timestamp	source_ip	source_port	destination_ip	destination_port	protocol	payload_hex
85	2024-10-08 01:54:23	10.101.102.215	54915	10.101.255.255	54915	UDP	007468655f50430000468f3b9702000060b77f5...
86	2024-10-08 01:54:23	20.187.186.89	NULL	10.101.102.215	NULL	TCP	1703030036bfa074f477871d3bff60d728aa9b2...
87	2024-10-08 01:54:23	10.101.102.215	NULL	20.187.186.89	NULL	TCP	170303003d9c7f927c1739e808e72b6dfa51ed2...
88	2024-10-08 01:54:24	10.101.102.215	54915	10.101.255.255	54915	UDP	007468655f50430000468f3b9702000060b77f5...
89	2024-10-08 01:54:24	10.101.102.215	NULL	103.28.54.101	NULL	TCP	1703030031d52e53de3559198273ba65a26864...
90	2024-10-08 01:54:25	10.101.102.215	54915	10.101.255.255	54915	UDP	007468655f50430000468f3b9702000060b77f5...
91	2024-10-08 01:54:26	10.101.102.215	54915	10.101.255.255	54915	UDP	007468655f50430000468f3b9702000060b77f5...
92	2024-10-08 01:54:27	10.101.102.215	54915	10.101.255.255	54915	UDP	007468655f50430000468f3b9702000060b77f5...
93	2024-10-08 01:54:27	10.101.102.215	32344	36.150.102.157	7826	TCP	1703030085286bb23fc7662c0733ad856f5411f...
94	2024-10-08 01:54:27	36.150.102.157	7826	10.101.102.215	32344	TCP	170303007fae455c804d10bf349a1e38194863b...
95	2024-10-08 01:54:28	10.101.102.215	54915	10.101.255.255	54915	UDP	007468655f50430000468f3b9702000060b77f5...
96	2024-10-08 01:54:29	10.101.102.215	54915	10.101.255.255	54915	UDP	007468655f50430000468f3b9702000060b77f5...
97	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	160301020001000 1fc0303f1c6cb8af28da040ff...
98	2024-10-08 01:54:29	113.240.75.252	NULL	10.101.102.215	NULL	TCP	160303005502000051030 3c29431385d5c0868...
99	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	140303000101160303002800000000000000000...
100	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	993d192ec040d623e1e0e9823476fb741c894ed...
101	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	d664b2a61e8c1698b82a0dec086e3dd0b0e938...
102	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	af9539759ff7876e77422f2666b5fc1bf5ad626b...
103	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	673064ae18fc23b7276dd710e1b9904a9bd89b...
104	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	b2ca1f758b6db90875aeeb35e3f2df0c3d3fe58c...
105	2024-10-08 01:54:29	10.101.102.215	NULL	113.240.75.252	NULL	TCP	c3f26b36fe2230e2c55826e6c1f74fbd4de44b24...
106	2024-10-08 01:54:30	113.240.75.252	NULL	10.101.102.215	NULL	TCP	17030300d72480573f70cc61ab1e7212d664f89...

rce_attacks 1

Figure 4. MySQL database page
图 4. MySQL 数据库页面

本模块还采用机器学习与统计分析，对攻击类型进行分类，涵盖 SQL 注入、XSS、远程代码执行(RCE)、DDoS、暴力破解等常见攻击方式。系统结合 IP 和端口词云分析，以可视化方式展示攻击热点 IP 和端口，便于管理员快速发现攻击重点目标。此外，所有分析数据均存储至 MySQL 数据库，如图 4 所示，支持历史数据检索与趋势对比，提高安全管理的可视化能力。通过全面的数据挖掘、可视化展示与攻击模式分析，本模块有效增强了系统的攻击感知能力，帮助管理员实现高效的网络安全监测和威胁评估。

3.3. 攻击预测模块

攻击预测模块采用支持向量回归(SVR)模型，原理如图 5 所示，基于蜜罐捕获的历史攻击数据，对未来可能发生的攻击行为进行预测。本模块的核心目标是识别高风险 IP、端口及攻击趋势，帮助管理员提前采取防御措施，提升系统的主动防御能力。系统首先对历史攻击数据进行预处理，包括攻击时间序列分析、IP 频率统计、端口关联性分析，然后通过特征提取与数据归一化，为 SVR 训练模型提供高质量的数据输入。SVR 通过核函数映射数据至高维空间，计算攻击发生的可能性，并输出未来一周内可能遭受攻击的 IP 和端口列表。

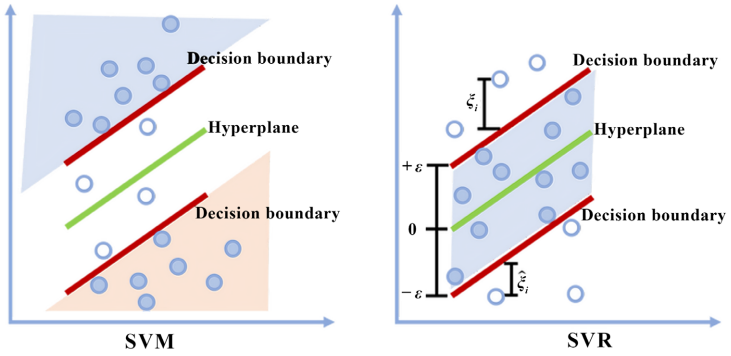

Figure 5. SVR model working principle
图 5. SVR 原理示意图

预测结果采用折线图、热力图和风险评分表进行可视化展示，直观呈现高风险 IP 的攻击趋势，帮助安全团队快速定位潜在威胁。此外，系统支持定期更新模型，利用最新的攻击数据优化 SVR 参数，提高预测精度。管理员可结合预测数据与实时攻击监测，调整防御策略，如加强特定端口的安全策略、屏蔽高风险 IP 或调整访问控制规则。通过机器学习驱动的攻击趋势预测，本模块有效提高了网络安全防护的前瞻性，使防御策略从被动响应转变为主动预防。

3.4. 数据可视化展示

数据可视化展示模块通过直观的图表和交互式界面，帮助管理员快速理解攻击数据，提升网络安全管理的效率。本模块基于 Streamlit 框架开发，系统主界面如图 6 所示，集成折线图、柱状图、热力图、词云图和地理分布图等多种可视化方式，展示蜜罐捕获的攻击行为。在捕获后还可以加载数据库中的界面回溯查询，如图 7 所示。

本模块的核心功能包括攻击趋势分析、攻击 IP 分布、端口攻击频率统计和机器学习预测结果可视化。攻击趋势分析采用折线图展示攻击次数随时间变化的情况，帮助管理员识别攻击高峰期。IP 分布图结合地理位置解析，直观展示攻击源的全球或区域分布情况，如图 8 所示。端口攻击频率统计通过词云图或柱状图呈现高频被攻击端口，为端口安全加固提供决策依据。攻击预测结果可视化部分采用热力图和风险评分表，展示未来高风险 IP 和端口的分布情况，如图 9 所示，便于管理员提前防御。

Figure 6. System dashboard main interface
图 6. 系统大屏主界面

最新导入的攻击数据

	ID	Timestamp	Source IP	Source Port	Destination IP	Destination Port	Protocol	Payload
0	3480296	2025-01-15 16:52:39	192.168.2.118	54915	192.168.2.255	54915	UDP	007468655f504300a0ad0bf6d2010000b0b61fcf1c0000000000000000000033270000
1	3480295	2025-01-15 16:52:39	192.168.2.118	49680	117.139.238.219	18695	TCP	000001504a9fd6cdc5ad17579ec030fed4d4a3b95b521e5e0652b42a43a69f01ff9dfd5a1
2	3480294	2025-01-15 16:52:39	192.168.2.118	50764	183.164.249.150	28679	TCP	00000150913ad1e8f26a8a07ac804fbef1e4e0b66a084a3e65c9b9e90c60fb3dccbeddaa
3	3480293	2025-01-15 16:52:39	192.168.2.118	54202	120.227.45.13	11217	UDP	e1f5629980009e7e8600204201508dda5fe61bb923261bbfcc489c8b57c0a8d2e456b40
4	3480292	2025-01-15 16:52:39	192.168.2.118	50775	117.150.80.87	4193	TCP	00000150badb8322bcbc5cc3e917815d688879d56121ccdd390a2bc1da1e46a02164db
5	3480291	2025-01-15 16:52:39	192.168.2.118	50763	222.213.97.73	9486	TCP	00000150f35c779936caa32ffec930bf7c0f3acf7d8620b7c88aca7dedd21e31b01cff2e72
6	3480290	2025-01-15 16:52:39	192.168.2.118	50760	120.227.197.189	24764	TCP	00000150c0cb2952b8a4d3a8a23f0dcf020bd22774db8677ad88d3b744bbe01503285bl
7	3480297	2025-01-15 16:52:39	120.227.45.13	11217	192.168.2.118	54202	UDP	083af821000001001b3b20429e7e
8	3348513	2025-01-15 16:52:39	192.168.2.118	50775	117.150.80.87	4193	TCP	00000150badb8322bcbc5cc3e917815d688879d56121ccdd390a2bc1da1e46a02164db
9	3348518	2025-01-15 16:52:39	120.227.45.13	11217	192.168.2.118	54202	UDP	083af821000001001b3b20429e7e
10	3348516	2025-01-15 16:52:39	192.168.2.118	49680	117.139.238.219	18695	TCP	000001504a9fd6cdc5ad17579ec030fed4d4a3b95b521e5e0652b42a43a69f01ff9dfd5a1
11	3348515	2025-01-15 16:52:39	192.168.2.118	50764	183.164.249.150	28679	TCP	00000150913ad1e8f26a8a07ac804fbef1e4e0b66a084a3e65c9b9e90c60fb3dccbeddaa

Figure 7. Database historical import
图 7. 数据库历史导入

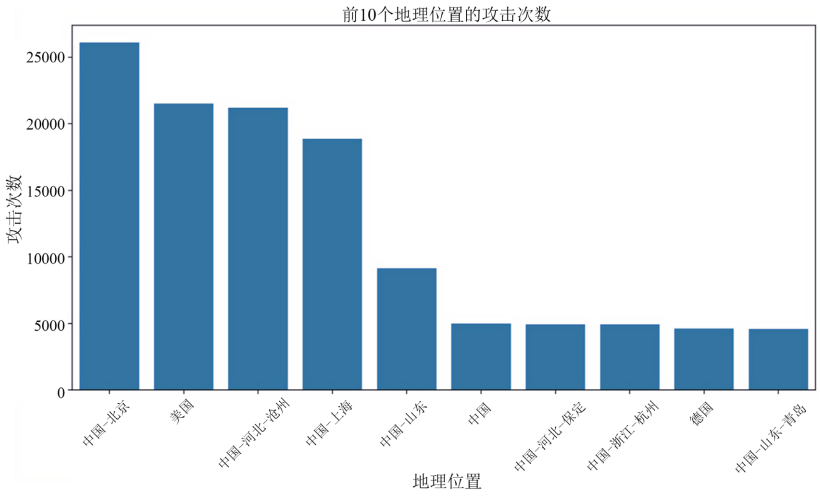

Figure 8. Geolocation source of attacks
图 8. 地理位置溯源

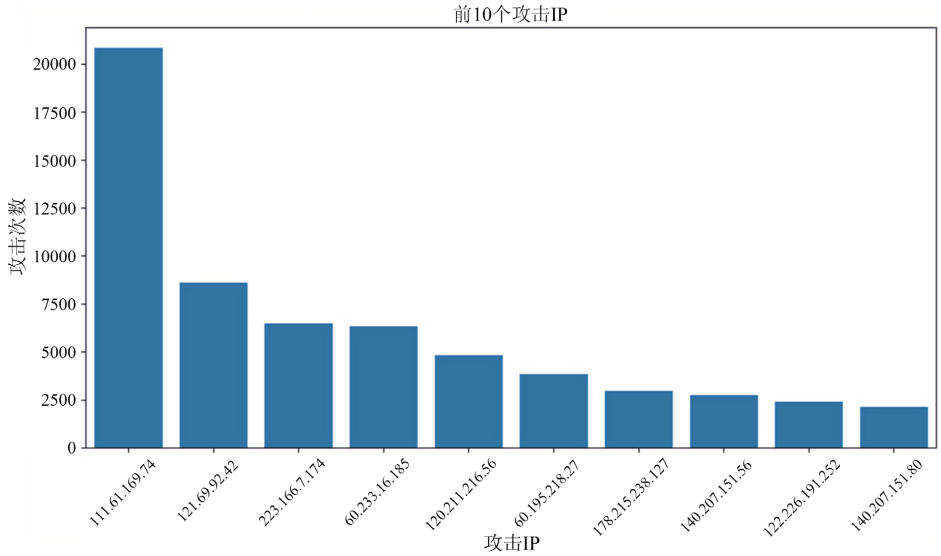

Figure 9. Attack IP statistics
图 9. 攻击 IP 统计

3.5. 性能比较

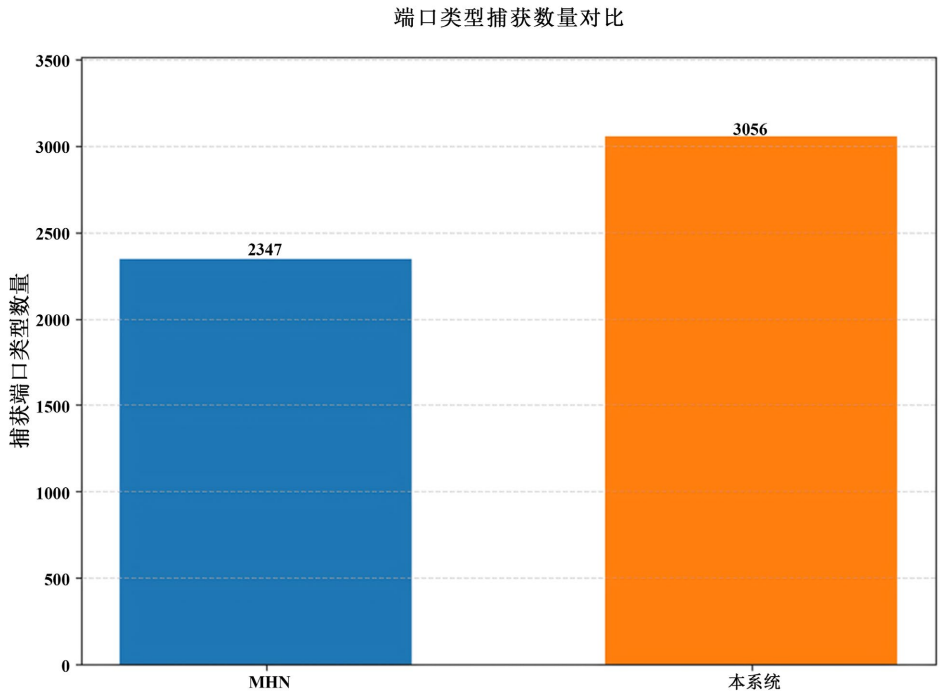

Figure 10. Performance comparison chart
图 10. 性能比较图

为了展示本系统的性能优势，与知名开源免费蜜罐 MHN 进行对比。对安装了 MHN 和本系统的服务器同时发送多次数据包，数据包报文为对伪造的 SQL 数据库登录界面进行 SQL 注入攻击，两种蜜罐都捕获了数据包并进行告警。但 MHN 并没有显示攻击类型，而本系统将攻击类型和攻击负载均显示出来。接着测试端口扫描及协议捕获类型，MHN 在承受攻击时一共捕获了 2347 个端口类型，本系统捕获了 3056

个端口类型。可以看出在类型分类方面要优于 MHN。具体对比如上图 10 所示。

4. 结论

本系统通过结合蜜罐监控、攻击数据分析、攻击预测等技术手段，提供了一种高效、可靠的网络攻击主动防御方案，显著提升了网络安全防护的实时性和精确性。系统的创新之处在于实时监测与攻击预测的结合，通过支持向量机回归(SVR)模型分析历史攻击数据，预测未来的攻击趋势。与传统的被动防御机制不同，本系统不仅能够在攻击发生时进行检测和响应，还能基于大数据分析和机器学习模型提前识别潜在的攻击目标，提高网络安全的主动防御能力。

本系统采用轻量化的 Streamlit 框架和 MySQL 数据库存储，能够在大规模网络环境下高效处理和管理攻击数据，保证了数据的实时处理与存取。通过动态可视化界面，管理员可以直观地了解攻击趋势、攻击源地理分布、攻击类型等信息，有效提升安全管理效率。实验结果表明，系统能够快速识别并预测如远程代码执行(RCE)、SQL 注入等常见攻击，提升了威胁响应效率和决策支持能力。

尽管如此，系统仍然面临一些挑战，如在复杂攻击场景下的误判率和预测精度问题。未来的研究可以通过优化 SVR 模型和增强数据处理算法，提高预测准确性和系统稳定性。此外，系统还可以扩展更多的攻击类型识别和深度学习预测功能，以适应更加复杂的网络环境和不断演化的安全威胁。本系统为网络攻击的主动防御提供了高效、可扩展的解决方案，具有广泛的应用前景，对于大规模网络环境中的安全测试和资产管理提供了强有力的支持。

基金项目

本文是江苏省大学生创新创业计划项目(xcx2024180)，徐州工程学院大学生创新创业项目(xcx2024190)的阶段性成果之一。

参考文献

[1] Stoll, C. (2005) The Cuckoo’s Egg: Tracking a Spy through the Maze of Computer Espionage. Simon and Schuster.
[2] Spitzner, L. (2002) Honeypots: Tracking Hackers. Addison-Wesley Professional.
[3] 张鑫杰. 基于蜜罐和深度学习的入侵检测技术研究[D]: [硕士学位论文]. 杭州: 浙江工商大学, 2021.
[4] 冀甜甜. 基于深度学习的智能恶意代码对抗技术研究[D]: [博士学位论文]. 北京: 北京邮电大学, 2022.
[5] 白雪擎. 基于蜜罐的网络入侵检测技术研究[D]: [硕士学位论文]. 长春: 长春工业大学, 2023.
[6] 杨书金. 基于 SVM 模型的恶意网页及 PDF 文档检测技术研究[D]. 赣州: 江西理工大学, 2014.
[7] 李珍珍. 基于蜜罐技术的网络安全防御系统的设计与实现[D]: [硕士学位论文]. 南京: 东南大学, 2019.
[8] 宋恺珉. 基于统计特征的网络入侵检测技术研究[D]: [硕士学位论文]. 南京: 南京邮电大学, 2015.