

**本科毕业设计（论文）**

题 目 网络安全评估数据可视化分析系统设计与实现

专业名称 计算机科学与技术

学生姓名 李宇轩

指导教师 潘炜

毕业时间 2023年7月

# 摘 要

互联网和网络通信技术的快速发展为人们的生产生活带来了重大变化，人们通过互联网获得了更多的信息和服务，而企业则利用网络实现了全球化的商业活动。然而，随着网络的普及和应用范围的扩大，网络安全问题也日益严峻，对网络的正常运行和隐私保护带来了巨大的挑战。

网络入侵检测作为一种重要的解决方案，已经成为保护网络安全的关键环节。传统的安全机制和防御策略已经不足以对抗规模化和自动化的网络攻击，这就要求我们采用新的方法和技术来保护网络免受恶意入侵的侵害。

在这方面，人工智能技术的应用成为了一个关键的突破口。利用人工智能构建的算法模型可以使人们更好地应对复杂、高强度的网络攻击，人工智能技术能够通过对大量的网络数据进行分析和学习，识别出异常的网络行为，并及时作出响应。这种基于人工智能的网络入侵检测系统具有较高的准确性和效率，能够帮助网络管理员及时发现和应对网络安全威胁，从而保护网络的安全运行。

此外，网络安全可视化也成为当前研究的热点之一。随着网络攻击手段的不断演变和复杂化，传统的文本或数字报告已经无法满足人们对网络安全状况的直观理解和快速反应的需求。因此，通过可视化的方式呈现网络安全数据和事件，可以更加直观地展示网络威胁的来源、形态和影响，帮助决策者更好地了解网络安全态势，并及时采取相应的措施应对威胁。

本文的主要工作内容如下：

（1）在CIC-IDS2017数据集上提出了一种针对poetscan和DDoS攻击的基于规则匹配的预测方法。通过对这两类攻击的特点总结以及针对数据集的特征研究，以数据集中的正常流量为基准，在部分特征上制定了相关规则，对预测数据进行流量检测分类。

（2）分离出部分攻击数据集，利用决策树机器学习方法，训练出用于流量分类检测的模型，从数据集中随机抽样部分数据进行模型预测，完成流量分类。

（3）将预测数据存入InfluxDB时序数据库，利用Grafana工具对预测数据进行可视化，实现系统目标。

关键词：网络安全评估，入侵检测，机器学习，CICIDS2017，可视化

# ABSTRACT

The rapid development of the Internet and network communication technology has brought significant changes to people's production and life. People have gained access to more information and services through the Internet, while businesses have achieved globalized commercial activities through the use of networks. However, with the popularization and expanded scope of networks, network security issues have become increasingly severe, posing significant challenges to the normal operation of networks and privacy protection.

Network intrusion detection, as an important solution, has become a critical aspect of protecting network security. Traditional security mechanisms and defense strategies are no longer sufficient to counter large-scale and automated network attacks, necessitating the adoption of new methods and technologies to protect networks from malicious intrusions.

In this regard, the application of artificial intelligence (AI) technology has become a key breakthrough. Algorithm models constructed using AI can better cope with complex and high-intensity network attacks. AI technology can analyze and learn from a vast amount of network data, identify abnormal network behaviors, and respond promptly. Such AI-based network intrusion detection systems have higher accuracy and efficiency, enabling network administrators to timely detect and respond to network security threats, thereby protecting the secure operation of networks.

Furthermore, network security visualization has also become a current research hotspot. With the continuous evolution and increased complexity of network attack techniques, traditional textual or numerical reports no longer meet the intuitive understanding and rapid response needs for network security conditions. Therefore, presenting network security data and events through visualization can more intuitively demonstrate the sources, forms, and impacts of network threats, helping decision-makers better understand the network security situation and take timely measures to address threats. The main work of this article is as follows:

1. A rule-based detection and prediction method is proposed for PortScan and DDoS attacks based on the CIC-IDS2017 dataset. By summarizing the characteristics of these two types of attacks and studying the features of the dataset, relevant rules are established based on the normal traffic in the dataset to classify and detect the predicted data.
2. A subset of attack datasets is separated, and a decision tree machine learning method is used to train a model for flow classification and detection. Random sampling of data from the dataset is used for model prediction to complete flow classification.
3. The predicted data is stored in the InfluxDB time-series database, and the Grafana tool is used for data visualization, achieving the objectives of the system.

**KEYWORDS:** network security assessment, intrusion detection, machine learning, CICIDS2017, visualization.

# 目 录

[摘 要 I](#_Toc139120005)

[ABSTRACT II](#_Toc139120006)

[目 录 IV](#_Toc139120007)

[第一章 绪 论 7](#_Toc139120008)

[1.1研究背景 7](#_Toc139120009)

[1.1.1 网络安全相关背景 7](#_Toc139120010)

[1.1.2 数据可视化相关背景 8](#_Toc139120011)

[1.2国内外研究现状 9](#_Toc139120012)

[1.2.1 入侵检测研究现状 9](#_Toc139120013)

[1.2.2 可视化研究现状 10](#_Toc139120014)

[1.3文章组织结构 11](#_Toc139120015)

[1.4研究意义和目的 12](#_Toc139120016)

[第二章 相关理论和技术 13](#_Toc139120017)

[2.1常见网络攻击类型 13](#_Toc139120018)

[2.1.1 端口扫描（PortScan） 13](#_Toc139120019)

[2.1.2 拒绝服务（DoS & DDoS） 14](#_Toc139120020)

[2.1.3 暴力破解口令入侵（BruteForce） 14](#_Toc139120021)

[2.1.4 浏览器攻击（Web Attack） 15](#_Toc139120022)

[2.1.5 僵尸网络（Botnet） 15](#_Toc139120023)

[2.1.6 渗透攻击 （Infiltration） 16](#_Toc139120024)

[2.1.7 心血漏洞（Heartbleed） 16](#_Toc139120025)

[2.2安全评估技术 16](#_Toc139120026)

[2.2.1 基于统计的异常检测 16](#_Toc139120027)

[2.2.2 基于规则的异常检测 17](#_Toc139120028)

[2.2.3 基于机器学习的异常检测 18](#_Toc139120029)

[2.2.4 基于数据挖掘的异常检测 18](#_Toc139120030)

[2.3网络安全相关数据集 18](#_Toc139120031)

[2.3.1 UNSW-NB15 19](#_Toc139120032)

[2.3.2 KDD CUP 1999 20](#_Toc139120033)

[2.3.3 CIC-IDS2017 20](#_Toc139120034)

[2.4可视化技术 24](#_Toc139120035)

[2.4.1 Telegraf 24](#_Toc139120036)

[2.4.2 InfluxDB 25](#_Toc139120037)

[2.4.3 Grafana 26](#_Toc139120038)

[2.5本章小结 27](#_Toc139120039)

[第三章 基于规则匹配和机器学习的检测与可视化 28](#_Toc139120040)

[3.1系统架构 28](#_Toc139120041)

[3.2基于规则匹配的入侵检测 28](#_Toc139120042)

[3.2.1 PortScan检测方法 29](#_Toc139120043)

[3.2.2 DDoS检测方法 30](#_Toc139120044)

[3.3基于机器学习的入侵检测 31](#_Toc139120045)

[3.4可视化方法 32](#_Toc139120046)

[3.4.1 PortScan可视化 32](#_Toc139120047)

[3.4.2 DDoS可视化 32](#_Toc139120048)

[3.4.3 其它类型攻击 33](#_Toc139120049)

[3.5本章小结 33](#_Toc139120050)

[第四章 系统设计与实现 34](#_Toc139120051)

[4.1工作流程 34](#_Toc139120052)

[4.2数据预处理 34](#_Toc139120053)

[4.2.1 数据清洗 34](#_Toc139120054)

[4.2.2 标签数值化 36](#_Toc139120055)

[4.2.3 特征选择 37](#_Toc139120056)

[4.2.4 数据标准化 39](#_Toc139120057)

[4.2.5 One-hot编码 39](#_Toc139120058)

[4.3模型训练 40](#_Toc139120059)

[4.4机器学习检测 41](#_Toc139120060)

[4.4.1 待预测数据生成 41](#_Toc139120061)

[4.4.2 模型数据预测 41](#_Toc139120062)

[4.5规则匹配检测 42](#_Toc139120063)

[4.6设备实时信息采集 43](#_Toc139120064)

[4.7数据入库 43](#_Toc139120065)

[4.8测试与结果 44](#_Toc139120066)

[4.8.1 实验环境 44](#_Toc139120067)

[4.8.2 数据库情况 45](#_Toc139120068)

[4.8.3 结果可视化 46](#_Toc139120069)

[4.8.4 实时数据发送测试 48](#_Toc139120070)

[4.8.5 准确性评判及分析 49](#_Toc139120071)

[第五章 总结与展望 51](#_Toc139120072)

[5.1已完成工作 51](#_Toc139120073)

[5.2未来展望 51](#_Toc139120074)

[参考文献 53](#_Toc139120075)

[致 谢 56](#_Toc139120076)

[毕业设计小结 57](#_Toc139120077)

# 绪 论

1.1研究背景

1.1.1 网络安全相关背景

近年来，随着计算机和网络的广泛应用，我们享受着数字化时代的便利和高效，然而也面临着新的威胁和挑战。网络恶意活动的数量显著增加，其对网络系统造成了严重威胁。

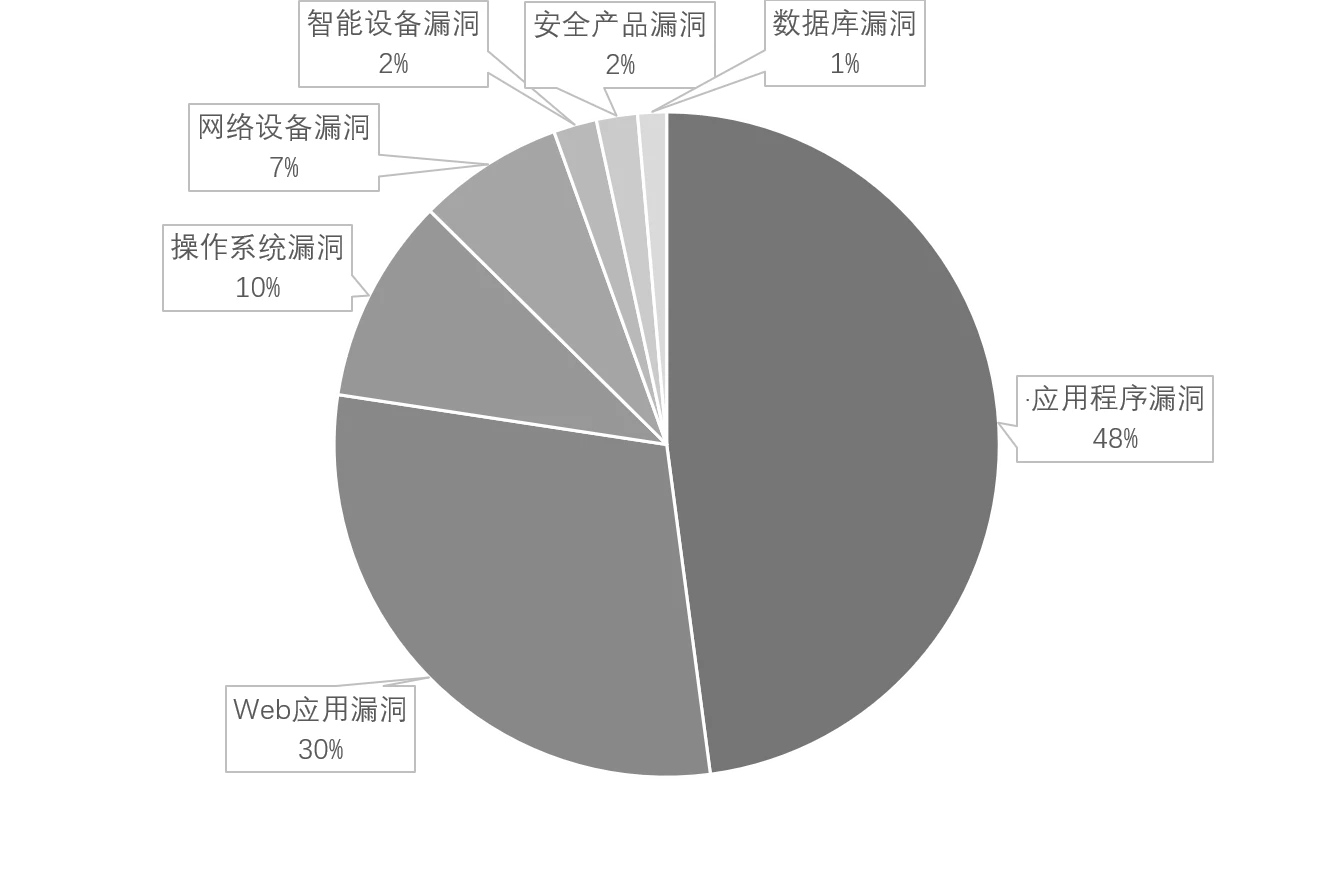


图 1–1 2020 年 CNVD 收录的安全漏洞数量占比按影响对象分类统计 （数据来源：CNCERT/CC）

据《2020年中国互联网网络安全报告》[1]显示，我国网络攻击呈现出急剧增加的趋势，主要的威胁形式包括分布式拒绝服务攻击（DDoS攻击）、高级持续性威胁（APT）、漏洞威胁以及网络黑灰产和工业控制系统等。具体情况如下：

1. DDoS攻击更加频发。

2020年我国党政机关和关键信息基础设施频繁受到DDoS攻击的困扰。黑客组织对300多个政府网站发起了超过1000次攻击，这些攻击波及了超过四分之三的目标网站。同时，物联网设备被黑客入侵并用于发动DDoS攻击的事件也大量涌现，每天平均约有220起攻击事件，峰值攻击流量超过10Gbit/s，相较去年同期增长超过40%。

1. APT攻击渗透重要行业。

APT组织常常使用钓鱼邮件作为攻击手段。2020年我国重要党政机关遭受钓鱼邮件攻击超过56万次，平均每月超过4万6千次。这些攻击由境外APT组织利用境外代理服务器作为跳板，对我国党政机关和重要行业进行持续的钓鱼邮件攻击。而这些攻击的范围不仅局限于党政机关、国防军工和科研机构，还扩展至基础行业、物联网和供应链等领域。

1. 网络系统面临漏洞威胁。

2020年国家信息安全漏洞共享平台接收了约14.1万条漏洞报告，其中通用软硬件漏洞的新增数量达到了16193个，同比增长了14%。这些漏洞威胁广泛覆盖了传统互联网和移动互联网领域，涉及到操作系统、办公自动化系统等软件，以及网络硬件设备和底层硬件。

这些漏洞的不断增加给网络和信息系统带来了更加严峻的安全威胁，攻击者可以利用这些漏洞来获取未授权的访问权限、窃取敏感信息、破坏系统稳定性等。由于漏洞数量的持续上升，加之不断发展的攻击技术和工具，网络和信息系统的安全形势变得更加复杂和严峻。

1. 工业控制系统存在安全问题。

随着工业互联网产业的发展，越来越多的工业企业将其业务迁移到云端，这导致更多的产品设备和信息系统暴露在互联网上，互联网侧的暴露面持续扩大。例如，据监测数据显示，2020年互联网上暴露的可编程逻辑控制器数量高达2,583台，同比增长了8.7%。而应用5G、工业物联网等技术为智能工业带来了便利的同时，也带来了一系列的安全隐患，例如信息泄露和智能设备接入认证管理问题。

物联网设备的灵活接入和广泛分布打破了传统工业控制系统的封闭性，引入了新的安全挑战。这些设备的智能化和互联互通使得工业控制系统面临着新的威胁，如远程入侵、数据篡改和服务中断等。由于物联网设备通常缺乏充分的安全保护机制，攻击者有可能利用其漏洞或弱点对工业控制系统进行攻击和渗透。

1.1.2 数据可视化相关背景

传统网络安全保障机制在当前大数据时代存在不足，难以有效对抗复杂的网络攻击。传统的杀毒软件、防火墙和入侵检测系统无法应对新的攻击类型和提前预测安全事件。同时，网络安全分析人员在处理网络异常时也遇到新的困难，如异构数据源和不断增长的数据量，以及新攻击类型和攻击复杂性的提高。此外，大量的漏报和误报，以及局部异常分析使得整体网络态势难以把握。

为了解决这些问题，网络安全可视化技术应运而生。它能够处理海量数据信息，捕获网络的全局态势，并以图形图像的形式展现高维数据。通过观察隐藏的模式，发现潜在的安全威胁，快速识别攻击和异常事件，甚至发现新的攻击类型。网络安全可视化技术可以将抽象的警报信息转化为直观的图像信息，并提供交互手段，帮助分析人员感知和理解网络安全数据。管理员可以方便地分析警报信息，了解网络动态和识别异常。这种技术已经当前已被引入到网络安全研究领域，并逐渐形成一个新的交叉研究领域。[1][2][3][4]

1.2国内外研究现状

1.2.1 入侵检测研究现状

入侵检测系统通过采集与计算机网络相关的检测数据，并经过数据处理建立数据特征，以实现对入侵的判别。研究人员已经将机器学习方法成功应用于入侵检测领域[5]，例如随机森林（Random Forest，RF）[6]、支持向量机（Support Vector Machine，SVM）[7]、K 近邻（K-Nearest Neighbor，KNN）[8]或人工神经网络（Artificial Neural Network，ANN）[9]等。相比传统的防火墙技术，入侵检测系统能够主动地监测和识别网络中的异常行为和恶意攻击，提供了一层额外的保护。

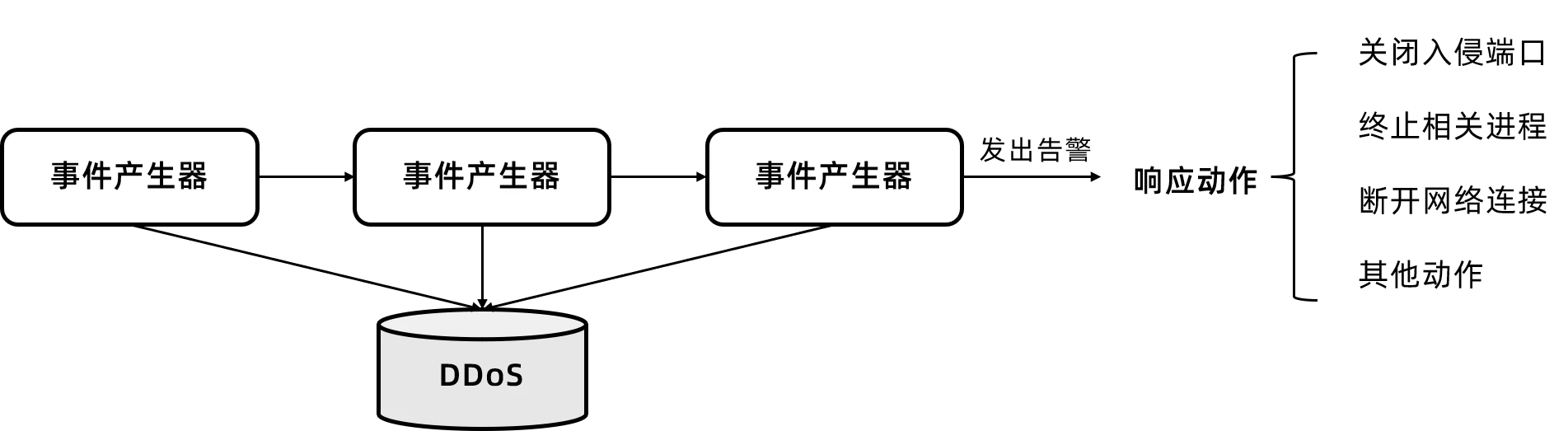


图 1–2 通用入侵检测系统框架

传统入侵检测技术在面对日益严峻的网络安全形势时存在多个弊端，需要不断研究和改进以适应新的挑战。首先，使用陈旧的数据集如KDD99、NSL-KDD或UNSW-NB15等，无法跟上网络入侵技术的发展速度。这些数据集仅包含过时的攻击模式和特征，无法准确地检测和识别新型的入侵行为。因此，研究人员需要更新数据集，收集和标记最新的攻击样本，以提高入侵检测系统的准确性和泛化能力。

其次，传统入侵检测技术更加注重准确率，而忽视了漏警率和虚警率。高虚警率会增加安全防护的成本，大量误报会占用人员和资源进行进一步调查和处理。因此，在研究入侵检测技术时，需要平衡准确率、漏警率和虚警率，以提高系统的综合性能和实用性。

另外，当前研究主要集中于正常与异常的二分类问题，无法为检测到入侵后的系统提供详细信息。针对具体病毒攻击类型的多分类研究较少，并且存在准确率低和虚警率高的问题。因此，需要开展更多针对具体攻击类型的多分类研究，深入分析各类入侵的特征和行为模式，以提高系统对不同类型攻击的检测能力和准确性。

为了改进传统入侵检测技术，研究人员可以探索使用更先进的机器学习和深度学习方法，例如深度神经网络、卷积神经网络和递归神经网络等，以提高检测的准确性和泛化能力。此外，引入行为分析和基于智能算法的动态入侵检测方法，可以更好地应对未知攻击和零日漏洞的威胁。

1.2.2 可视化研究现状

20世纪90年代中期开始，网络安全可视化（Network Security Visualization）作为一个新兴领域，正在越来越多地受到关注。它通过将网络安全数据和态势以图形化、可视化的方式呈现，提高了对网络安全风险的识别和理解能力[10]。相对于传统的网络安全日志分析软件或方法，网络安全可视化能够更好地处理和展示大量的网络安全数据，使得人们能够更直观地掌握网络安全状况。

通过可视化技术，人们可以更全面地了解网络中的安全事件和攻击行为，从而更及时地做出反应和采取措施。此外，网络安全可视化还能够提供交互式的功能，用户可以根据自己的需求进行数据的筛选、聚焦和深入分析，进一步加深对网络安全的认识。

国内外对网络安全可视化的研究和应用已经取得了一些成果，并成为重要的研究议题。越来越多的研究者和从业者开始关注和借助网络安全可视化技术，用于监测和分析网络攻击、评估网络安全风险、优化安全策略等方面。同时，随着人工智能和大数据等技术的发展，网络安全可视化也将迎来更多创新和应用，为网络安全领域带来更多的可能性。

1. 基于流量的可视化

网络安全事件如端口扫描、蠕虫扩散和拒绝服务攻击通常会对网络流量产生明显的异常影响，通常表现为一对一、一对多或多对一的数据传输模式。网络流量可视化可以帮助网络安全分析人员快速发现并应对网络攻击，该技术使用网络数据包的各种属性，如源IP、目的IP、源端口、目的端口、协议和时间等信息进行分析。例如，nvisionip[11]是一种网络数据流量可视化工具，它能够以直观的方式展示系统的状态，提高网络安全分析人员对整个安全态势的感知能力。Pgvis3d[12]结合了2D和3D可视化技术，为网络流量监控信息提供了交互式的展示方式。这种工具不仅能够同时显示针对特定主机和网段的扫描事件，还能够以图形化的形式展示网络流量的分布情况。

这些网络可视化技术通过分层的方式呈现网络数据，有效地帮助网络分析人员检测网络内部和外部、以及内部之间的数据流动情况。通过可视化工具，网络分析人员能够更加深入地了解网络的实时状态，及时识别潜在的安全威胁，并采取相应的安全措施。

1. 基于端口的可视化

黑客在进行网络攻击或入侵之前通常进行信息收集，包括目标主机或网络的扫描，以确定系统状态、运行服务和操作系统类型，并寻找系统漏洞。端口扫描是最常见的攻击方法，用于确定目标主机开放的端口。Portvis[13]通过多视图和交互方式，帮助分析人员监测和识别网络中潜在的安全事件，利用可视化技术展示网络信息，并提供多个视图来辅助监测和发现潜在的安全事件。

1. 基于入侵检测的可视化

网络分析人员广泛使用基于网络的入侵检测系统来辨识和对抗各种网络攻击，例如DDoS攻击、网络蠕虫和木马等。这些系统通过实时比对当前网络数据包与已知攻击类型签名数据库的信息，并根据匹配结果判断是否触发警报。然而，由于误报率的存在，需要采用一种可视化工具来提高入侵检测系统的准确性。

Snortview[14]是一种基于图元方法的网络安全可视化工具，旨在实时分级显示snort报警信息。它通过可视化的方式帮助网络分析人员快速理解和评估报警事件的严重程度，从而降低误报率，并提高对真实威胁的警觉性。

目前，国外已经启动了多个安全可视化项目，如SIFT、idswatch、Network Eyes和GA-IDS等。这些项目致力于开发先进的可视化技术，以加强对网络安全事件的感知和理解。虽然国内在网络安全领域的理论和工程实践方面取得了重大进展，但网络安全可视化的理论基础和关键技术仍存在未探索和研究的空白，进一步的探索和研究是推动网络安全可视化领域发展的关键。通过深入研究，我们可以不断改进可视化工具的效能，提高网络安全分析人员对威胁的察觉能力，并为网络安全防护提供更强大的支持。

1.3文章组织结构

本文共分为五章，各章主要内容如下：

第一章，绪论。主要介绍本文的研究背景与意义，总结了网络安全及其可视化方面的国内外研究现状，简要介绍了文本的研究内容，并给出了本文的组织结构。

第二章，相关理论和技术。介绍常见的网络攻击类型以及相应的评估技术，同时对一些常用的数据集进行了介绍，尤其对本文实验使用的CICIDS2017数据集进行了详细介绍。最后对一种网络安全信息可视化技术进行了说明。

第三章，基于规则匹配和机器学习的检测与可视化。首先对CICIDS2017的几种攻击类型的检测方法进行了阐释，分别是基于规则匹配的PortScan和DDoS，以及通过机器学习进行预测的其它攻击类型。其次对这几类攻击的可视化指标和方法进行了说明。

第四章，系统设计与实现。本章利用前文介绍的方法及理论，基于CICIDS2017数据集，开发了一种利用机器学习和规则匹配判断网络攻击类型的安全评估系统，同时利用InfluxDB以及Grafana实现了可视化。

第五章总结了本文所做的工作，并做了进一步的工作展望。

1.4研究意义和目的

随着因特网技术的不断发展，网络空间资源已成为国家重要的信息基础设施。然而，网络空间安全却面临着重大挑战。不法分子利用信息技术进行网络攻击，危及国家和公众利益。因此，识别和阻止不断涌现的、多变的网络攻击已成为国家战略和社会需求。

传统的网络安全技术往往难以满足新型攻击的快速识别和防御需求。在这样的背景下，网络安全可视化系统应运而生。这些系统通过将复杂的网络数据可视化展示，帮助分析人员快速发现异常行为和潜在的攻击模式，并提供预警和相应的防御措施。

研究和开发网络安全可视化系统可以提高网络异常检测的准确性和效率，降低误报率和漏报率，从而增强网络安全防护能力。这对于提升网络安全防护水平、保护国家和公众利益具有重要意义。实现对网络异常行为的及时识别、快速响应和有效防御是网络安全可视化系统的目标，通过这样的系统，我们可以确保网络空间的安全和稳定运行，应对不断增长的网络威胁，保护国家的重要信息基础设施和公众的个人信息安全。

# 相关理论和技术

本章对网络安全评估及可视化中涉及到的技术进行了详细的分析与研究，包括网络攻击的典型类型和应用于攻击检测领域的机器学习算法，只有在此基础上，才能充分把握网络攻击检测技术的重点。

2.1常见网络攻击类型

在计算机和计算机网络领域，攻击行为包括破坏、揭露、修改或使软件或服务失去功能，以及未经授权访问或窃取计算机数据[15]。这些网络攻击可能对用户的网络环境造成异常，并构成对网络安全的威胁。而异常指的是在正常数据中出现具有不同特征的新数据。这些特征可能是由黑客入侵主机、盗用邮箱信息、窃取情报等因素引起的。当网络环境受到攻击时，通常会出现与正常流量不符的异常行为，如非正常的数据流、异常的连接模式或协议使用，以及异常的数据量或频率。这些异常特征可以是攻击者入侵系统、进行未经授权的活动或窃取敏感信息的迹象。根据数据的不同类别，异常可以分为三类。

1. 点异常：指在一个数据集中，某个或少数几个数据与其他数据显著不同，可以单独标识为异常。这种异常通常是由于突发事件或异常情况导致的，例如，对于工业数据来说，如果一辆新能源汽车在正常情况下每天消耗5kw/h的电量，但某一天的消耗量突然变为10kw/h，那么这个数值10就是一个点异常。
2. 上下文异常：指某个数据在特定的上下文环境中与通常情况的变化趋势有明显区别，这种异常需要考虑数据的背景和环境因素，只有在特定的上下文中才被视为异常。例如，春节期间，铁路客运量一般会极大提高，若某地在这期间客运量却明显降低，就可能存在上下文异常。
3. 集体异常：指整体数据的变化与通常情况存在明显差异，可以看作是一组数据的集体行为异常。这种异常表示整个数据集合的行为与平均或预期的行为不一致。例如在铁矿石价格中，若某一时期铁矿石价格持续走低，可能是由于国际开采量过高引起的异常情况，就可以认为存在集体异常。

网络攻击具有多种类型，每种类型都有其特定的行为和目的。其中，拒绝服务攻击旨在通过产生大量无用的流量使网络系统中断，导致网络无法正常运行。而端口扫描攻击则用于探测可进入的服务和潜在漏洞。在进行攻击检测技术研究之前，了解各种网络攻击的机理是必要的，这有助于我们理解攻击者的行为模式和目的，从而有效地应对和防御这些威胁。

2.1.1 端口扫描（PortScan）

端口扫描是一种常见的网络侦察技术，攻击者使用端口扫描工具来了解目标系统的服务和安全漏洞。通过分析反馈信息，端口扫描能够获取目标系统的特征和漏洞信息[16]。而端口扫描器则是一种专门用于确定系统开放端口的工具。它可以进行水平扫描和垂直扫描两种方式。水平扫描指对不同计算机的同一端口进行有目的性的多次扫描，而垂直扫描则是对同一计算机的不同端口进行有目的性的多次扫描[17]。

通过端口扫描攻击，攻击者可以深入了解目标系统，找到潜在的漏洞和弱点。这为他们进一步入侵目标系统提供了有价值的信息。因此，保护网络安全和及时修补系统漏洞至关重要，以防止恶意攻击者利用端口扫描等手段对系统进行侵害。

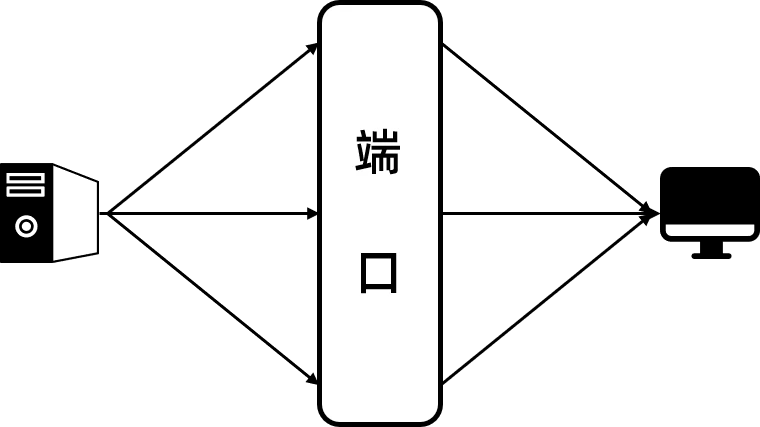
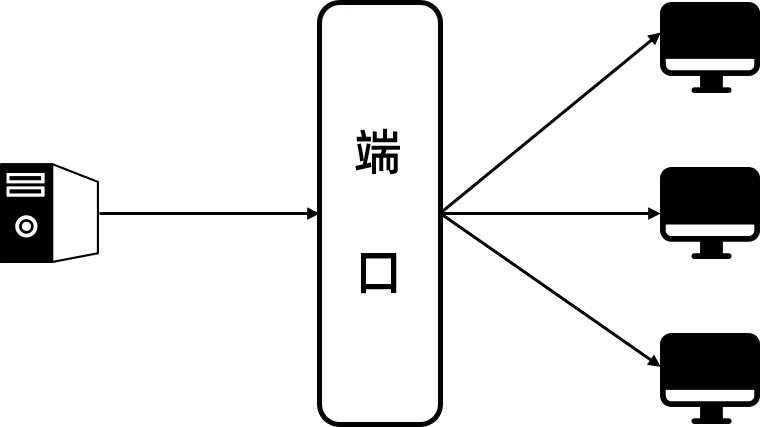


图 2–1 端口水平扫描 图 2–2 端口垂直扫描

2.1.2 拒绝服务（DoS & DDoS）

拒绝服务攻击（DoS）是指攻击者利用大量连接尝试来增加目标系统的负载，从而使其无法正常提供服务。这种攻击会消耗目标系统的资源，导致系统无法处理正常的请求。分布式拒绝服务攻击（DDoS）是更加复杂和具有威力的攻击形式，它利用多个攻击源同时发起攻击，进一步加剧了目标系统的负荷。通过分散攻击流量和难以追踪攻击源，DDoS攻击使得防御变得更加困难[18]。

CICIDS2017模拟HTTP拒绝服务攻击，攻击者使用诸如Slowloris和LOIC等工具来发起攻击。Slowloris攻击通过保持与服务器的连接打开，阻止其他连接的建立，从而占用服务器资源，导致服务的可用性下降。

拒绝服务攻击的目的是使目标系统无法正常运行，造成服务的中断或降级。攻击者可能出于各种动机进行此类攻击，包括报复、勒索或纯粹的恶意行为。

2.1.3 暴力破解口令入侵（BruteForce）

暴力破解攻击是指攻击者通过反复尝试不同的密码组合来获取系统或服务的访问权限。攻击者使用自动化软件执行大量的密码尝试，通常针对弱用户名和密码组合进行入侵[19]。为了实施暴力破解攻击，攻击者使用各种工具和技术。其中一些常见的暴力破解工具包括Hydra、Medusa、Ncrack、Metasploit模块和Nmap NSE脚本。另外，还有一些用于破解密码哈希的工具，如Hashcat和Hashpump。这些工具利用字典攻击、暴力破解和其他密码猜测技术来尝试破解密码并获取访问权限。

CICIDS2017数据集模拟了暴力破解攻击的场景。该数据集使用了位于Kali Linux计算机上的FTP和SSH作为攻击者计算机，并以Ubuntu14.0系统作为受害计算机并使用了一个包含9000万个单词的密码词典，用于尝试破解目标系统的密码。

2.1.4 浏览器攻击（Web Attack）

基于浏览器的网络攻击是一种利用浏览器破坏计算机系统的方法，攻击者通常以合法但易受攻击的网站为起点，试图利用浏览器中的漏洞将恶意软件注入用户系统[20]。

CICIDS2017使用了Damn Vulnerable Web App (DVWA)作为被攻击的Web程序，该程序是一个PHP/MySQL Web应用程序，旨在帮助安全专业人员在合法环境中测试其技能。攻击行为通常包括对网站进行漏洞扫描，然后利用易受攻击的网站进行各种类型的Web攻击，如SQL注入、命令注入和不受限制的文件上传。为了自动化XSS和BruteForce攻击，CICIDS2017采用了Selenium框架开发的自动化代码。

通过利用浏览器的漏洞，攻击者可以通过访问受感染的网站将恶意软件强制输入用户系统，从而可能导致系统被完全控制、敏感信息被窃取或遭受其他形式的损害。

2.1.5 僵尸网络（Botnet）

僵尸网络是指利用受害者计算机进行攻击或滥用在线服务的网络。僵尸网络由以下组成部分构成：1) 多个僵尸计算机，2) 命令与控制（Command & Control）服务器，3) 僵尸主机[21]。

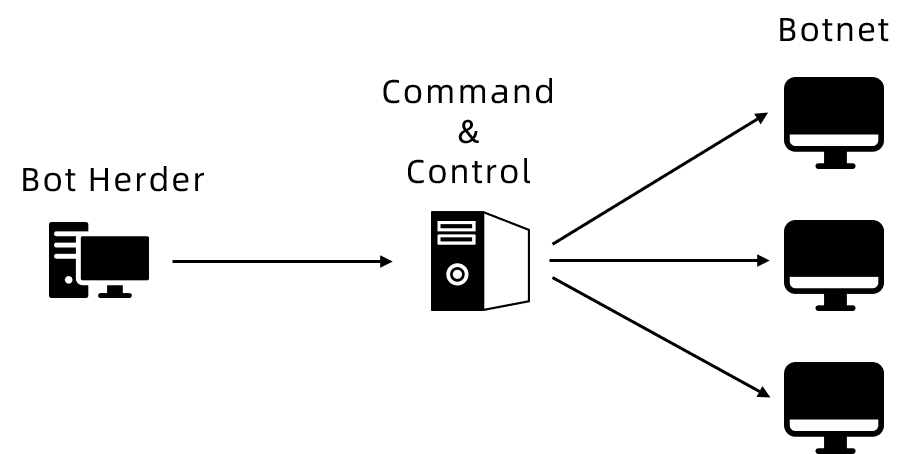


图 2–3 僵尸网络示意图

CICIDS2017数据集对使用Zeus和Ares作为工具的僵尸网络攻击行为进行了模拟。Zeus被用于窃取银行信息和安装勒索软件，而Ares用于执行远程命令、文件操作和键盘记录等活动。攻击者通过感染计算机并定期请求屏幕截图来利用这两个不同的僵尸网络。这种行为可能用于监视受害者的活动、窃取敏感信息或执行进一步的攻击。

2.1.6 渗透攻击 （Infiltration）

网络渗透攻击中，攻击者通过发送恶意文件给受害者的电子邮件，利用应用程序漏洞在受害者计算机上安装后门，以获取对系统的持久访问权限。一旦攻击者成功安装后门，他们会利用受感染计算机在内部网络中进行扫描，寻找其他易受攻击的漏洞，并尝试利用这些漏洞进一步扩大攻击范围[22]。

CICIDS2017数据集模拟了这种从内部渗透到网络的攻击行为，其中包括通过电子邮件发送恶意文档以及利用Metasploit框架中的漏洞。一旦攻击者成功渗透到受害者计算机，他们会执行后门程序，这样就能够进行各种网络攻击，如IP扫描、全端口扫描和使用Nmap进行服务枚举。

2.1.7 心血漏洞（Heartbleed）

Heartbleed是一个openssl软件库中公开揭露的安全漏洞，于2014年4月被揭示。这个漏洞使攻击者可以在TLS/DTLS加密通信中读取服务器内存中的敏感信息，包括私钥、用户凭证和其他敏感数据。攻击者利用Heartbleed发送特制的心跳请求消息，而实际数据长度却小于指定长度。通过这种方式，攻击者可以从服务器中获取敏感信息，导致信息泄露的风险增加。

Heartbleed漏洞的影响范围非常广泛，因为许多网站和网络服务都使用openssl来实现安全通信。据估计，全球数百万个网站受到这个漏洞的威胁。这使得许多用户的个人信息、密码和其他敏感数据面临潜在的危险。

CICIDS2017使用Heartleech工具来模拟Heartbleed漏洞，检索服务器内存中的数据，并研究其对系统的影响。这种模拟有助于深入了解Heartbleed漏洞的工作原理和潜在风险，以便采取适当的安全措施来保护系统和数据。

2.2安全评估技术

目前，主流的入侵检测系统主要分为两种类型：基于网络的入侵检测系统和基于主机的入侵检测系统。它们的区别在于部署位置和数据源。基于网络的入侵检测系统部署在网络中，数据源是网络数据包；而基于主机的入侵检测系统部署在主机上，数据源是主机的审计日志。而常见的异常检测方法包括统计、规则、数据挖掘和机器学习。这些方法用于分析网络数据包，并检测其中的异常行为，以识别潜在的入侵活动。

在本文中，主要关注基于网络的入侵检测系统，并设计相关实验。

2.2.1 基于统计的异常检测

在统计方法中，入侵检测系统通过跟踪系统中的对象（如网络流量、主机活动等）的动态行为来生成配置文件。这些配置文件描述了对象的正常行为模式，包括其使用的协议、端口、频率、大小等信息。

当入侵检测系统检测到新的事件或对象时，它会将其与配置文件进行比对。比对的结果可以给出该事件或对象的异常程度值，用于判断是否存在潜在的入侵活动。较高的异常程度值表示较大的可能性是恶意或异常行为，需要进一步的分析和响应。通过比对检测数据与配置文件，统计方法能够帮助入侵检测系统识别出与正常行为模式不一致的行为，从而提供潜在的入侵检测和警报[24]。

统计方法的优点是它可以通过自适应学习来识别正常用户的行为特征，从而比专家更敏锐地察觉到异常。这使得入侵检测系统能够更早地进行预警并采取相应的处理措施。

然而，统计方法也存在一些缺点。在学习正常用户行为特征时，如果有网络入侵活动发生，统计方法可能将其误认为是正常流量并进行学习。这可能导致最终的入侵检测将该种入侵方式视为用户的正常行为，从而无法正确地识别入侵活动。

统计方法需要在学习和识别过程中精确地区分正常行为和异常行为，以避免误判和漏报的情况发生。因此，在设计和使用入侵检测系统时，需要考虑综合多种方法和技术，以提高检测的准确性和可靠性[25]。而入侵检测系统所面临的挑战之一是确定应该监控哪些数据，以及学习哪些性能来实现完美的正常与异常划分。入侵检测系统通常需要结合其他方法，如行为分析、基于规则的检测、机器学习等技术，以提高检测的准确性和覆盖范围[26]。

2.2.2 基于规则的异常检测

规则匹配基于预定义的规则集，用于检测特定的恶意行为或攻击模式。这些规则通常由安全专家或研究人员根据已知的攻击特征和漏洞编写。基于规则的检测工作原理如下：

1. 规则定义：安全专家根据已知的攻击行为或恶意活动编写规则，规则通常包含与特定攻击相关的模式、行为或特征。
2. 规则匹配：入侵检测系统通过监控网络流量、主机日志或其他数据源，将收集到的数据与预定义的规则进行匹配。
3. 检测与警报：如果数据与任何规则匹配，入侵检测系统将触发警报，指示可能存在恶意活动或攻击。

基于规则的检测方法的优点是其易于理解和实施，可以通过简单的逻辑进行判断。同时，其具有较高的可定制性，安全专家可以根据特定的需求和环境编写自定义规则，以适应特定的威胁和攻击情景。另外，基于规则的检测还可以进行实时监测，可以快速匹配和检测恶意活动，使得入侵检测系统能够及时发现和响应潜在的攻击。

然而，基于规则的检测方法也存在一些限制。首先是它依赖已知的攻击特征，规则是基于已知的攻击模式编写的，对于新型的、未知的攻击可能无法有效检测。其次，如果规则定义不准确或过于广泛，可能会导致误报情况的发生，影响系统的可用性和操作效率。

2.2.3 基于机器学习的异常检测

网络入侵检测算法旨在区分恶意访问和正常访问，以维护网络安全。其中最简单的方法是通过对相应流量进行模式匹配，然后判断该流量是否是正常流量。该问题的本质是一个分类问题，即将其转化为恶意和正常访问的二分类问题。如果进一步确定恶意访问的类型，可以将该问题转化为多分类问题。其优点明显，基于模型预测可以很好地识别和适应用户的正常行为，同时无法像统计方法一样被入侵者利用。

机器学习系统通过经过一段时间的学习，能够提升在特定任务上的性能表现。相较于传统的统计方法，机器学习更加注重对数据的处理和应用，通过不断进行预训练和更新模型的权重，可以提高其对新型攻击的识别能力[27]。

机器学习模型的学习和分类性能在许多领域已经得到验证，利用机器学习的方法可以自适应地学习数据中用户的正常行为的相关特征。其优点是检测的准确率较高，能够检测出之前未遇到的入侵行为，而且机器学习算法众多，能够覆盖很多异常检测场景的需求。

然而，机器学习也有一定的局限性，例如训练数据决定了机器模型的性能，这与基于统计的方法一样，决定哪些类型、哪些信息的数据作为训练数据是模型入侵检测性能的关键[26]。

2.2.4 基于数据挖掘的异常检测

数据挖掘技术在异常检测方面扮演着重要的角色，有助于提升异常检测模型的性能表现。在异常检测中，一种常见的搜索算法是遗传算法，其具有灵活性和鲁棒性的特点，能够在多个尺度范围内寻找最优解[28]。除此之外，聚类是另一种广泛应用于异常检测的方法，其通过对样本进行分组和归类，能够自动发现高维数据中的分类规律。聚类在异常检测中可以采用未标记的正常和攻击样本数据进行模型训练，也可以使用普通样本通过训练模型生成活动的配置文件。通过聚类后形成的簇大小可以用来判断样本数据的类别，大簇通常代表正常数据，而小簇则可能代表攻击数据[29]。

通过数据挖掘技术，异常检测模型能够从大量的数据中发现潜在的异常模式和行为，进而提高对异常的识别能力。这种方法可以帮助安全专业人员更准确地检测和应对不断变化的网络攻击和异常行为，提升整体的网络安全水平。

2.3网络安全相关数据集

网络安全数据集在评估和改进网络安全技术、算法和解决方案方面起着关键作用。它们为研究人员、安全专家和组织提供了一个标准化和实际的基础，用于测试和验证安全性能，发现新的威胁，并提供更好的保护措施。

1. 训练和测试模型：网络安全数据集提供了丰富的网络流量和入侵行为数据，可用于训练和测试入侵检测系统、安全分析算法和其他网络安全模型。使用真实的网络数据进行训练可以提高模型的准确性和鲁棒性。
2. 评估算法性能：这些数据集可以作为评估不同入侵检测算法性能的基准。研究人员和安全专家可以使用这些数据集来比较不同算法在检测和识别各种网络攻击方面的性能。通过对算法的准确性、召回率、误报率等指标进行评估，可以选择最适合特定应用场景的算法。
3. 发现新的威胁：网络安全数据集中包含多种类型的网络入侵行为和攻击模式。研究人员可以通过对这些数据进行分析和挖掘，发现新的威胁和攻击技术。通过深入分析数据集，可以识别新的入侵模式和漏洞，并改进现有的安全防护措施。
4. 验证安全解决方案：这些数据集可以用于验证和评估安全解决方案的有效性。例如，网络设备厂商可以使用这些数据集来测试其防火墙、入侵检测系统和其他安全产品的性能。通过在真实的网络流量上进行测试，可以验证这些解决方案的功能和可靠性。

下面介绍一些网络安全领域常用的数据集。

2.3.1 UNSW-NB15

UNSW-NB15是一种广泛使用的网络入侵检测数据集，用于评估和研究入侵检测系统的性能和效果。该数据集由悉尼科技大学（University of New South Wales）的网络安全实验室创建，并于2015年发布。其主要特点如下：

1. 数据收集：UNSW-NB15数据集是通过捕获和记录真实网络流量而创建的。数据来自悉尼科技大学的实际网络环境，包括正常的网络活动和多种类型的网络攻击行为。
2. 数据规模：该数据集包含超过2千万个网络连接记录，覆盖了近一个月的网络流量。数据集中包含了全面的网络活动，包括多种类型的攻击行为和正常的网络传输。
3. 攻击类型：UNSW-NB15数据集包含了43种不同类型的网络攻击，涵盖了常见的入侵行为，如拒绝服务（DoS）、扫描、恶意软件和僵尸网络等，每种攻击类型都经过了详细的分类和标记。
4. 数据特征：该数据集提供了大量的网络流量特征，包括传输协议、源IP地址、目标IP地址、源端口、目标端口、流量统计指标、包长度等。这些特征可以用于构建入侵检测系统，并分析和识别各种攻击行为。
5. 数据集划分：UNSW-NB15数据集根据时间划分为训练集和测试集。训练集包含了大部分的数据记录，用于模型的训练和参数调优。测试集用于评估模型的性能和泛化能力。

通过使用UNSW-NB15数据集，研究人员和安全专家可以进行入侵检测算法的评估和比较，提升入侵检测系统的性能，并探索新的入侵模式和威胁。该数据集的丰富性和实际性使其成为网络安全研究和实践中重要的资源。

2.3.2 KDD CUP 1999

KDD CUP 1999是一个经典的网络入侵检测数据集，被广泛应用于研究和评估入侵检测系统。它是1999年国际知识发现与数据挖掘竞赛（Knowledge Discovery and Data Mining, KDD）的数据集，由美国加州大学欧文分校（University of California, Irvine）的计算机科学系提供。其主要特点如下：

1. 数据收集：KDD CUP 1999数据集是通过模拟一个仿真网络环境进行数据收集而创建的。数据集模拟了一个真实的网络环境，并包含了各种网络连接和传输。
2. 数据规模：该数据集包含约4百万个网络连接记录。这些记录涵盖了多种类型的网络活动，包括正常的网络传输和不同类型的入侵行为。
3. 攻击类型：数据集中包含多种类型的网络攻击，包括拒绝服务（DoS）、远程登录（R2L）、用户到root（U2R）和探测（Probing）等。每种攻击类型都经过了详细的分类和标记。
4. 数据特征：KDD CUP 1999数据集包含大量的网络连接特征，如传输协议、源IP地址、目标IP地址、源端口、目标端口、持续时间、传输字节数等。这些特征可用于构建入侵检测系统，并分析和识别各种攻击行为。
5. 数据集划分：KDD CUP 1999数据集被划分为训练集、测试集和评估集。训练集用于模型的训练和参数调优，测试集用于评估模型在未见过的数据上的性能，评估集则用于最终的性能评估和比较。

KDD CUP 1999数据集的丰富性和实用性使其成为入侵检测系统研究和评估的重要基准。研究人员和安全专家可以使用这个数据集来开发新的算法、评估系统性能，并提供更强大的网络安全保护措施。

2.3.3 CIC-IDS2017

CICIDS2017 (Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset 2017)[30]是一个广泛使用的网络入侵检测数据集，用于评估和研究入侵检测系统的性能。该数据集由加拿大网络安全研究院提供，包含了正常行为和14种典型的入侵网络数据流，符合真实的网络场景。

CICIDS2017数据集提供了PCAP数据包文件和对应的网络流量特征数据CSV文件。它涵盖了Windows系统、Linux系统以及Mac OSX系统的流量数据，并具有丰富的协议类型。

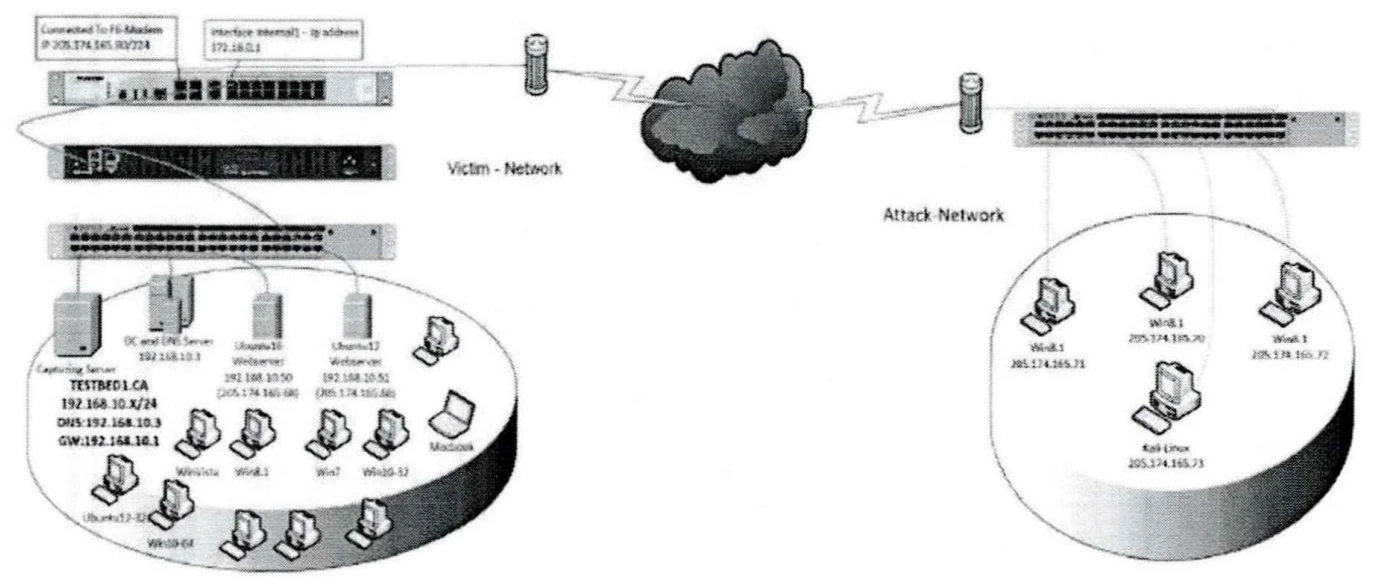


图 2–4 形成CICIDS2017攻击网络模型架构

以前的IDS数据集无法涵盖构建可靠基准数据集所需的10条标准，包括：

1. 完整的网络配置：包括调制解调器、防火墙、交换机、路由器和多种操作系统（例如Windows、Ubuntu和Mac OSX）的组合。
2. 全面的流量内容：包括用户配置的代理、受害者网络中的12台不同计算机以及来自攻击网络的真实攻击。
3. 标记的数据集：包含了经过标记的正常和攻击数据。
4. 完整的交互：覆盖了两个不同网络和Internet之间的通信，包括内部局域网和不同内部局域网之间的通信。
5. 全面捕获：使用镜像端口（如分流系统），将所有流量完全捕获并记录在存储服务器上。。
6. 可用协议：支持所有常见的可用协议，例如HTTP、HTTPS、FTP、SSH和电子邮件协议 。
7. 攻击多样性：涵盖了基于2016年mcafee报告中最常见的攻击类型，例如Web攻击、暴力破解、DoS、DDoS、渗透、Heartbleed、僵尸网络和扫描。
8. 异构性：在攻击执行期间，捕获来自主交换机的网络流量，以及所有受害计算机的内存转储和系统调用。
9. 特征集：使用cicflowmeter从生成的网络流量中提取了80多个网络流量特征，并将网络流量数据集提供为CSV文件。

(10)元数据：包括数据集的时间、攻击、流量和标签等元数据信息。

CICIDS2017数据集基于真实场景收集，用于进行网络安全和异常检测的研究。该数据集中的正常流量部分通过脚本模拟人们日常的操作行为，例如发送电子邮件等常见活动。为了生成包含多种协议的正常行为流量数据包，模拟了25个用户的日常行为，包括HTTP、HTTPS、FTP等协议。而网络攻击流量数据部分则包含各种恶意样本，如拒绝服务攻击、SSH暴力破解、端口扫描以及Web攻击中的SQL注入、XSS等。这些攻击会导致用户IP地址的计算机产生相应的网络流量。数据集提供了一个基于真实场景的测试环境，有助于更好地理解和应对各种网络安全威胁。

表2-1 CICIDS2017数据集攻击标签说明及占比

| **攻击类别** | **说明** | **数据条数** | **占比** |
| --- | --- | --- | --- |
| BENIGN | 正常流量 | 2273097 | 91.795% |
| DoS | 攻击者旨在降低网络资源 | 252661 | 10.221% |
| PortScan | 攻击者试图发送不同目标端口的数据包，以获取与受害计算机相关的信息，如操作系统类型和运行服务 | 158930 | 6.429% |
| DDoS | 攻击者使用多台计算机共同操作来攻击一台受害者计算机 | 128027 | 5.196% |
| Patator | 暴力攻击 | 13835 | 0.560% |
| Web Attack | 与网页有关的攻击 | 2180 | 0.088% |
| Bot | 受害者计算机的安全性遭到攻击者使用木马程序的破坏，导致攻击者能够控制和操纵网络中的所有计算机，攻击者可以远程利用和管理这些计算机 | 1966 | 0.079% |
| Infiltration | 攻击者利用渗透方法和工具，未经授权地渗透并获取对网络系统数据的完全访问权限 | 36 | 0.001% |

采集时间从2017年7月3日星期一上午9点开始，到7月7日下午5点结束，为期五天。除了7月3日是完全正常的网络数据之外，其余四天都包含不同病毒类型产生的攻击数据。

表2-2 CICIDS2017数据采集情况

| **日期** | **网络活动** | **大小** |
| --- | --- | --- |
| 2017年7月3日 | 正常 | 11.0G |
| 2017年7月4日 | 正常 + 暴力破解 | 11.0G |
| 2017年7月5日 | 正常 + DoS | 13.0G |
| 2017年7月6日 | 正常 + Web攻击 + 渗透 | 7.8G |
| 2017年7月7日 | 正常 + 僵尸网络 + 端口扫描 + DDoS | 8.3G |

在CICIDS2017数据集中，每一行数据都代表一个数据流。然而，将单个流量包视为一次通信行为是不准确的，因为同一IP地址和端口之间的通信往往是连续且多次的。为了更准确地表示通信行为，我们将具有相同IP地址和端口组合，并且在一定时间段内间隔不超过某个阈值的主机之间的流量归类为同一通信行为。通过这样的方式，我们能够更好地反映实际通信情况，将连续的通信行为作为一个整体进行分析，从而提高对网络流量的理解和处理能力。

CICIDS2017对pcap数据包进行分析，利用数据流中的各种信息来提取特征，包括数据包数量、数据包长度、速率、持续时间和端口等数据流量指标。通过使用pcap分析工具，将提取的特征根据时间和攻击活动类型进行分类，并将它们按时间顺序存储在八个CSV文件中。流量的标记是基于主要时间戳、源IP、目标IP和端口的匹配。这个过程中将具有相同攻击时间、攻击IP、端口和协议的流量划分为同一组，并为该组流量添加相应的标签。通过这种方法，数据流可以得到有效的标记和分类，从而为后续的入侵检测分析提供基础。

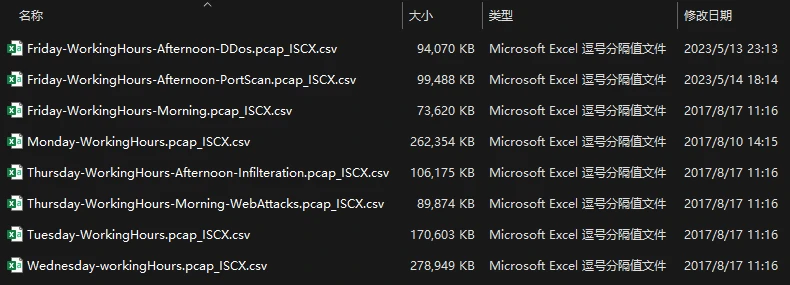


图 2–5 CICIDS2017数据文件

标记的流量数据文件共85列（最后一列为攻击类别），用于机器学习的流量数据文件有79列，缺失的六列分别是：

* Flow ID
* Source IP
* Source Port
* Destination IP
* Protocol
* Timestamp

因为Flow ID和Timestamp不是常规的数值型数据，因此去除它们可以简化计算和分析过程。IP地址和源端口与确定攻击类别无关，因为攻击者可以使用不同的IP地址和源端口进行攻击。相比之下，协议与攻击类别存在较大的相关性，因此去除协议可以提高机器学习算法分类结果的可信度。通过消除这些不相关的特征，可以简化数据集，进而提高入侵检测算法的准确性和效率。

2.4可视化技术

在网络安全中应用可视化技术可以更直观地观察和分析变化趋势、异常值和攻击模式。可视化分析有助于提供对攻击行为的全面视角，以便更好地采取相应的安全措施和防御策略。

本文基于Telegraf + Influx DB + Grafana的架构方法，用于搭建数据可视化和监控平台。与传统的监控方式相比，这种架构系统简单易用，无需编辑脚本，只需获取监控数据即可自动抓取并实时展示，操作简单，方便进行运行和维护。下面对这三种工具进行简单介绍。

2.4.1 Telegraf

Telegraf是一个插件驱动的服务器代理，用于收集和报告各种指标。它能够与容器和系统直接集成，从中提取指标、事件和日志数据。Telegraf的设计目标是简化指标收集和传输的过程，提供高性能和可扩展性。它支持多种输入插件和输出插件，可以从不同的数据源获取指标数据，并将数据发送到目标系统进行存储或展示。Telegraf具有以下几类特点：

1. 多种输入插件：Telegraf支持多种输入插件，可以从不同的来源采集数据，如系统指标（CPU、内存、磁盘等）、网络流量、日志文件、消息队列等。这使得Telegraf可以灵活地适应各种数据源的需求；
2. 数据处理和过滤：Telegraf具有数据处理和过滤功能，可以对采集到的数据进行转换、聚合、过滤和标准化等操作。这样可以提高数据的质量和准确性，使数据更具有可用性；
3. 插件生态系统：Telegraf拥有丰富的插件生态系统，用户可以根据需求选择合适的插件来支持特定的数据源或目标系统。插件可以提供额外的功能和灵活性，使Telegraf更易于集成和扩展；
4. 高性能和低资源消耗：Telegraf被设计为高性能的指标收集代理，具有低的资源消耗。它使用Go语言开发，具有并发处理能力和轻量级的特性，可以高效地处理大规模的指标数据；
5. 输出到InfluxDB：Telegraf与InfluxDB紧密集成，可将采集到的指标数据直接发送到InfluxDB时序数据库进行存储和查询。这种集成简化了数据流的管理和分析，提供了强大的时序数据处理能力。

Telegraf内部设计了4种类型的插件。它们必须按照特定的顺序进行组合：1）输入插件；2）处理插件；3）聚合插件；4）输出插件。

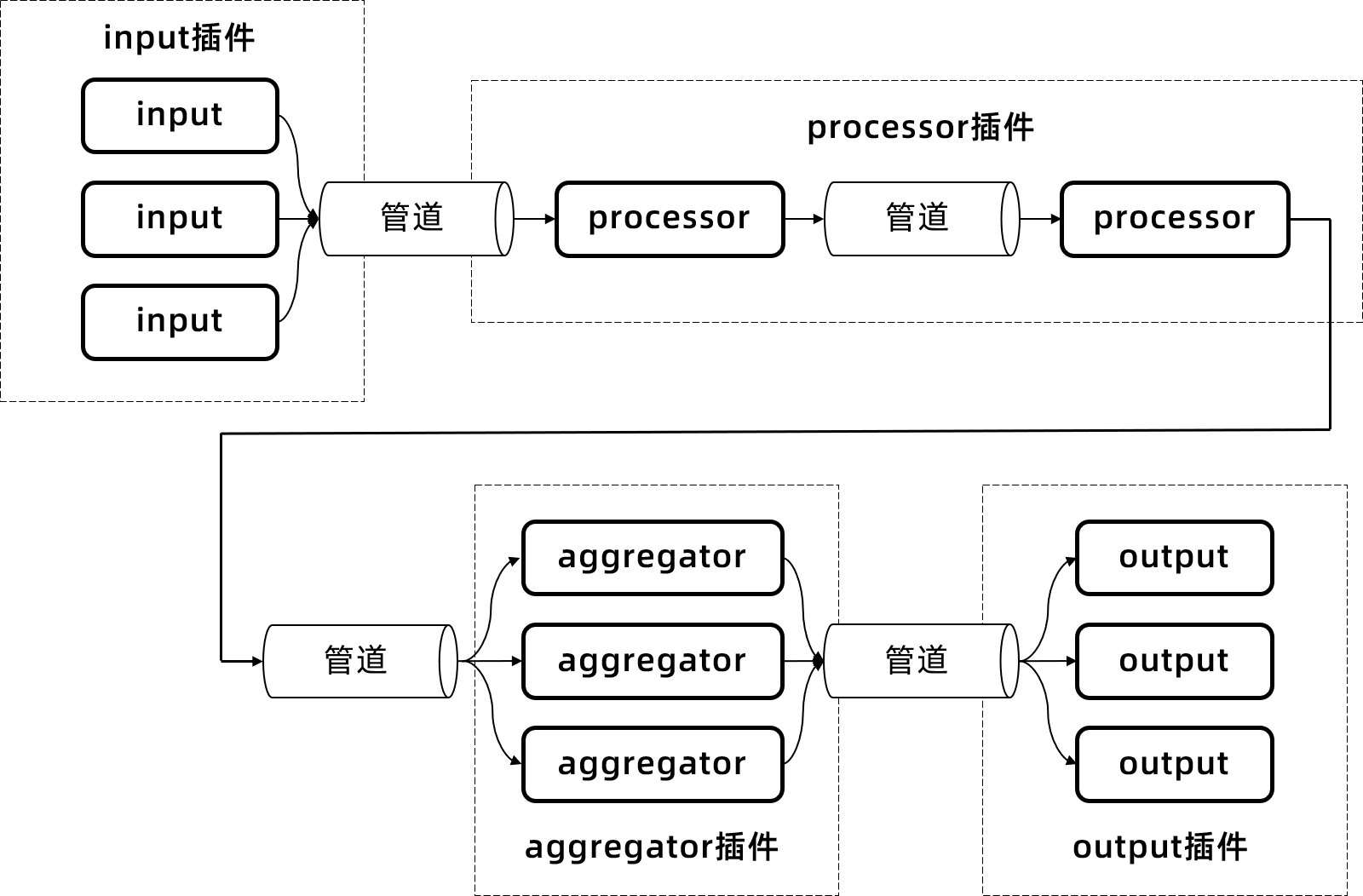


图 2–6 Telegraf插件执行顺序

* 所有的input插件会将数据放入同一个管道。
* 所有的processor插件会按先后顺序传递数据（在配置文件中必须显示地指定顺序，否则Processor之间会以随机顺序组合）
* Aggregator前的管道会把数据复制给所有的Aggregator插件，不过Telegraf还为插件们设计了指标过滤器，插件可以选择性地接收部分数据。
* Output前的管道也会将数据复制给所有的output组件，不过同样可以使用过滤器组件选择性地接收。

2.4.2 InfluxDB

InfluxDB是用Go语言编写的一个开源分布式时序、事件和指标数据库，它的目标是专门用于高效地存储和检索时间序列数据。InfluxDB具有自包含的特性，无需依赖外部组件或数据库，被设计用于处理具有时间戳的大规模数据集，例如传感器数据、应用程序指标、日志数据等。InfluxDB具有以下几类特点：

1. 时序数据存储：InfluxDB专注于存储时间序列数据，它使用时间戳作为主要索引，并以时间为基准进行数据分片和存储。这种设计使得InfluxDB能够高效地处理大量的时间序列数据，具有出色的写入和查询性能；
2. 标签和字段：InfluxDB使用标签（Tags）和字段（Fields）的概念来组织数据。标签是用于标识和过滤数据的键值对，相当于关系数据库中的key，而字段则包含实际的数据值。这种结构使得数据可以按照不同的维度进行查询和聚合，提供了灵活而强大的数据处理能力；
3. 数据保留策略：InfluxDB允许用户定义数据的保留策略，即数据存储的时间范围。可以根据需求配置不同的保留策略，自动删除过期的数据，以控制数据库的存储空间和性能；
4. 插件生态系统：InfluxDB拥有丰富的插件生态系统，用户可以根据需求选择适用的插件来扩展数据库的功能。插件可以提供与其他工具和系统的集成，例如数据可视化、报警通知等。

写入该数据库的数据需遵循InfluxDB行协议的格式标准，具体如下：

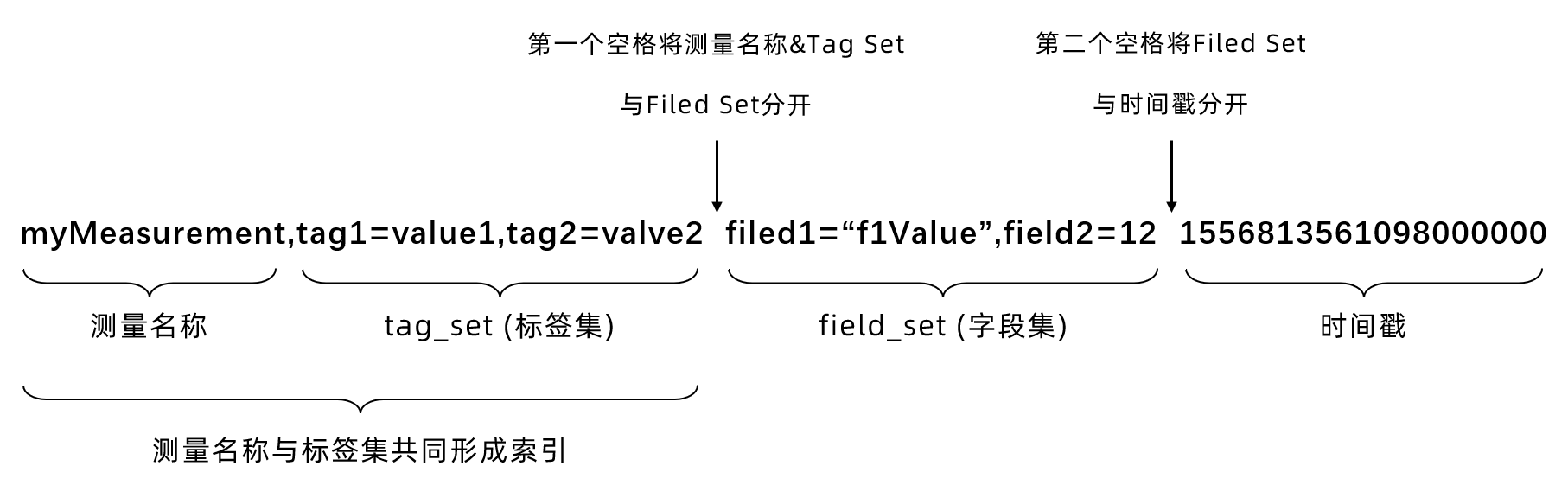


图 2–7 InfluxDB行协议

2.4.3 Grafana

Grafana是一种开源的数据可视化和监控平台，用于实时展示和分析数据。它提供了丰富的可视化选项和灵活的数据查询功能，可以从不同的数据源中获取数据并将其以直观和可交互的方式呈现。Grafana作为开源数据可视化工具，具有以下优点：

1. 多数据源支持：Grafana支持连接多种数据源，包括时序数据库（如InfluxDB、Prometheus）、关系型数据库（如MySQL、PostgreSQL）、日志文件（如Elasticsearch、Splunk）等。这使得用户能够从不同的数据源中获取数据，并在同一个界面中进行统一的数据可视化和分析。
2. 丰富的可视化选项：Grafana提供了多种图表和仪表盘组件，包括折线图、柱状图、饼图、仪表盘、地图等。用户可以根据需求选择适合的图表类型，并通过配置参数和样式来自定义图表的外观和行为。
3. 灵活的数据查询语言：Grafana支持灵活的数据查询语言，如ProSQL、InfluxSQL、SQL等，用户可以使用这些语言从数据源中检索数据，并在图表中进行展示。这些查询语言提供了丰富的聚合、过滤和计算功能，使用户能够根据需要对数据进行处理和分析。
4. 告警和通知：Grafana具有强大的告警功能，用户可以设置基于数据的告警规则，并在触发规则时发送通知。通知可以通过电子邮件、Slack、Webhook等方式进行发送，及时通知用户关键数据的变化和异常情况。
5. 用户权限和认证：Grafana支持用户权限和认证机制，可以通过角色和权限设置来管理用户对仪表盘和数据的访问权限。这使得用户能够控制和限制不同用户组的数据访问和操作能力。

2.5本章小结

本章介绍了网络安全评估及可视化中涉及的相关理论和技术。首先，介绍了常见的网络攻击类型，包括端口扫描、拒绝服务、暴力破解口令入侵、浏览器攻击、僵尸网络、渗透攻击和心血漏洞。然后，探讨了安全评估技术，包括基于统计的异常检测、基于规则的异常检测、基于机器学习的异常检测和基于数据挖掘的异常检测。接着介绍了一些网络安全相关的数据集，如UNSW-NB15、KDD CUP 1999和CIC-IDS2017，用于评估和研究入侵检测系统的性能。最后，讨论了可视化技术在网络安全中的应用，包括Telegraf、InfluxDB和Grafana等工具的使用。

总结起来，本章提供了关于网络安全评估和可视化的基本概念和相关技术，为理解和应用网络安全领域的方法和工具提供了基础。

# 基于规则匹配和机器学习的检测与可视化

本章对CICIDS2017的几种攻击类型的检测方法进行了阐释，分别是基于规则匹配的PortScan和DDoS，以及通过机器学习进行预测的其它攻击类型，另外还对这几类攻击的可视化指标和方法进行了说明。

3.1系统架构

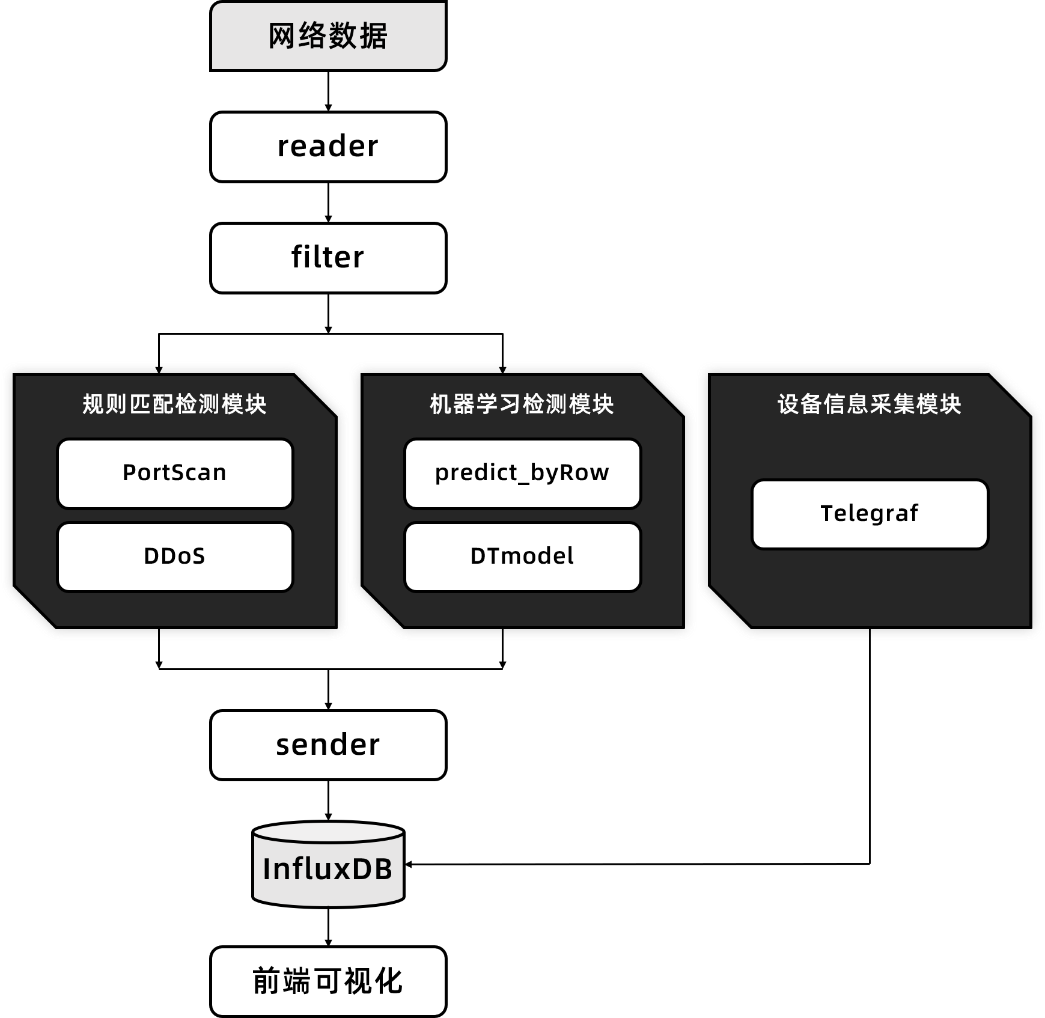


图 3–1 系统架构图

3.2基于规则匹配的入侵检测

CICIDS2017数据集中共包含85类标签，部分标签的具体含义如下表所示：

表3-1 CICIDS2017标签含义

|  |  |  |  |
| --- | --- | --- | --- |
| **标签** | **含义** | **标签** | **含义** |
| Flow ID | 流标识符，用于唯一标识每个网络流量 | Source IP | 源IP地址 |
| Source Port | 源端口号 | Destination IP | 目标IP地址 |
| Destination Port | 目标端口号 | Protocol | 协议类型 (TCP, UDP, ICMP等) |
| Timestamp | 时间戳，表示流量的发生时间 | Flow Duration | 流持续时间 |

本部分结合CICIDS2017中的各个指标，根据各类攻击的特点，提出PortScan、DDoS攻击基于统计预测的检测方法。

3.2.1 PortScan检测方法

PortScan攻击主要针对网络中的主机和服务的端口进行大量的扫描和探测，以获取目标主机的开放端口和服务信息，其目的是探测目标主机的漏洞和弱点，以便进行后续的攻击或侦察。PortScan通过扫描目标主机的端口来获取信息，通常不涉及直接向目标发起攻击流量。

根据前文介绍，PortScan攻击可分为水平扫描和垂直扫描。水平扫描是对不同主机的同一端口进行扫描；而垂直扫描则是对同一主机的不同端口进行扫描，在扫描过程中目的主机IP数与目的端口数的比值远小于1[31]，即:

CICIDS2017数据集中的该类攻击均为垂直扫描，结合其各类流量特征，可以从以下几个指标判断流量是否为PortScan攻击：

1. Total Fwd Packets、Total Backward Packets：对前向和后向数据包的数量进行监测，如果存在极少的前向和后向数据包，即明显小于正常链接的均值，并且目标端口在不同的IP地址之间频繁变化，可能是进行端口扫描的行为；
2. Fwd Packet Length Max、Fwd Packet Length Min和Bwd Packet Length Max、Bwd Packet Length Min：端口扫描通常会发送特定长度的数据包进行探测，如果存在特定长度范围内的数据包，则可能是端口扫描活动，通过分析后向数据包的长度范围，可以判断是否存在端口扫描活动；
3. Fwd Header Length：端口扫描通常使用简单的探测技术，发送的数据包头部长度可能较短且大量重复，因此可以通过监测包头长度判断是否存在端口扫描活动。

表3-2 BENIGN与PortScan标签在部分数据上的平均值

| **标签** | **BENIGN** | **PortScan** | **判断依据** |
| --- | --- | --- | --- |
| Total Fwd Packets | 16.8 | 3.4 | 端口扫描攻击的数据包量显著小于正常流量 |
| Total Backward Packets | 20.9 | 3.5 |
| Fwd Packet Length Min | 17.4 | 10.3 | 端口扫描攻击的包长度范围通常为固定值，因此可以通过判断其包长大小来分辨流量 |
| Fwd Packet Length Max | 232.8 | 81.1 |
| Bwd Packet Length Min | 34.8 | 27.5 |
| Bwd Packet Length Max | 1220.0 | 185.8 |
| Fwd Header Length | 264.7 | 91.9 | 端口扫描攻击的数据包以探测为主，因此其头部长度通常小于正常包 |

若某个流量的上述各个值均异常，则可判断数据中某条流量是否为PortScan攻击。

3.2.2 DDoS检测方法

DDoS攻击与其他类型的网络攻击相比具有以下特点：

1. 大规模：DDoS攻击通常涉及大量的攻击源和攻击流量，可以造成目标系统或网络的完全瘫痪。攻击者利用大量被恶意软件感染的计算机，同时向目标发起大量的请求，超过目标系统的处理能力，导致服务不可用。
2. 分布式：DDoS攻击利用多个攻击源发起攻击，这些攻击源可以位于全球各地，使得攻击更难追踪和阻止。攻击者可以通过操纵大量被感染的计算机或设备，协同发起攻击，使得防御变得更加困难。
3. 持久性：DDoS攻击可以持续一段时间，从几分钟到几天甚至更长。攻击者可以不断调整攻击策略和攻击源，以持续对目标进行攻击，导致长时间的服务中断和损失。

针对以上特点，结合CICIDS2017数据集的各类流量特征，可以从以下几个指标判断流量是否为DDoS攻击：

1. Total Fwd Packets、Total Backward Packets和Total Length of Fwd Packets、Total Length of Bwd Packets：这些指标均与数据量大小有关，若这些指标远低于正常值，则可能为DDoS攻击；
2. Flow Duration：监测流的持续时间，如果持续时间较长且有大量的流量，可能是DDoS攻击；
3. Destination Port：监测目标端口，如果短时间内有针对主机端口的大量连接尝试或异常的目标端口活动，可能是DDoS攻击；
4. Flow IAT Mean、Flow IAT Std：该指标表示流内平均包间隔时间，若该值远大于正常值，则该流量可能为DDoS攻击为了保持攻击链接而产生。

表3-3 BENIGN与DDoS标签在部分数据上的平均值

| **标签** | **BENIGN** | **DDoS** | **判断依据** |
| --- | --- | --- | --- |
| Total Fwd Packets | 16.8 | 4.4 | 这几类指标远低于正常值，该类流量通过少量数据包长时间占用网络资源 |
| Total Backward Packets | 20.9 | 3.2 |
| Total Length of Fwd Packets | 734.2 | 31.9 |
| Total Length of Bwd Packets | 36428.0 | 7373.7 |
| Flow Duration | 11661081.0 | 16955856.6 | 流量持续时间远大于正常值，说明该类流量长时间占用网络资源 |
| Flow IAT Mean | 845457.5 | 1881553.6 | 平均包间隔时间远大于正常值，导致网络连接大量处于闲置状态 |
| Flow IAT Std | 1601626.1 | 5111941.3 |

若某个流量的上述各个值均异常，则可判断数据中某条流量是否为DDoS攻击。

3.3基于机器学习的入侵检测

在机器学习中，分类是一个重要的任务。当将实例分为两个类别时，称为二分类问题。而当将实例分为三个或更多类别时，则称为多分类问题。分类任务的目标是通过学习从输入数据到类别标签之间的映射关系，对新的未标记数据进行分类预测。在本研究中，将流量数据其分为七个类别，详细分类结果可参考第四章内容。

决策树是一种用于分类任务的树状结构。每个分支代表可能具有某一类别特征的集合，非叶节点表示不同类别的相同特征，而叶节点则表示具体的类别。决策树的分类过程始于根节点，对每个子节点的属性进行测试，并根据属性值选择相应的分支，一直进行到达叶节点，叶节点则代表最终的分类结果。

将70%的数据作为训练数据，30%的数据作为测试数据。分类测试效果如下，在CICIDS2017数据集中，决策树算法展现了更好的综合效果。而深度学习等方法主要适用于图像语音等单个大型文件的分类。所以之后的测试均使用该机器学习算法[31]。

表3-4 各种机器学习模型的测试效果表

|  |  |  |
| --- | --- | --- |
| **模型** | **检出率/(%)** | **误报率/(%)** |
| Naive Bayse | 90.2 | 3.6 |
| Decision Tree | 91.9 | 2.91 |
| Random Forest | 91.9 | 2.93 |
| Logistic Regression | 89.2 | 3.1 |

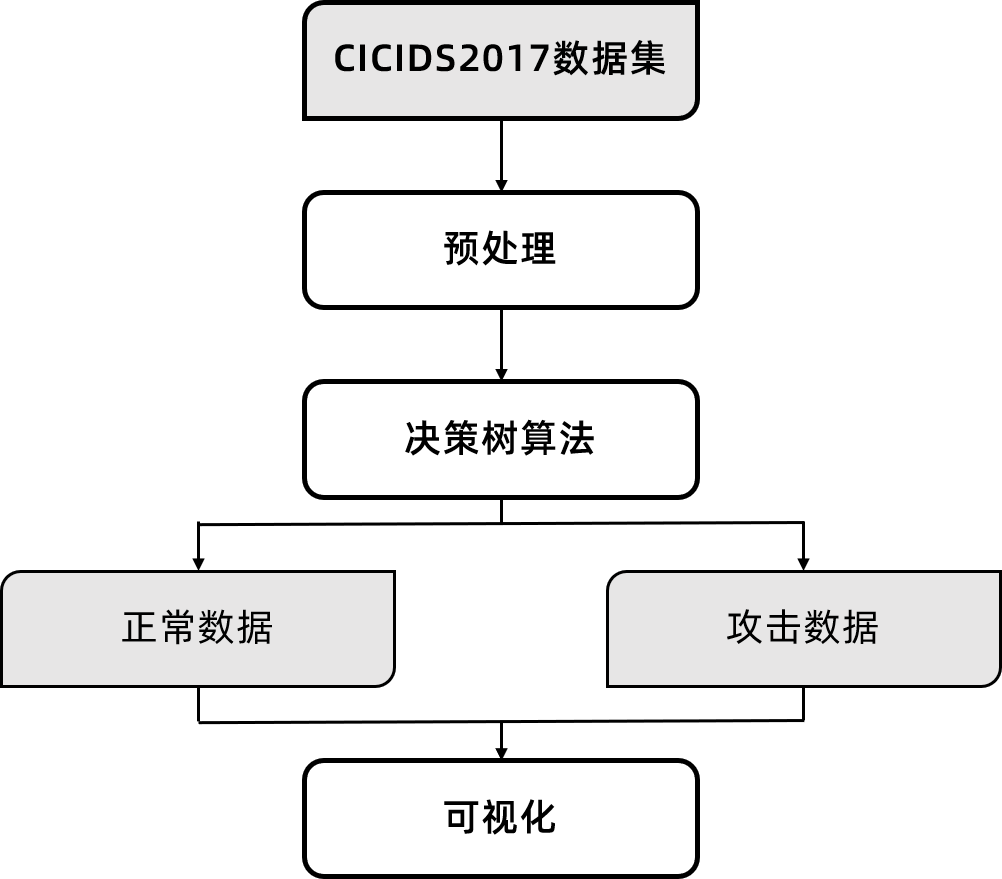


图 3–2 机器学习检测流程

3.4可视化方法

3.4.1 PortScan可视化

根据前文中提到的PortScan监测方法，可以将以下信息进行可视化处理：

* 1. 扫描IP及被扫描端口；
  2. 被扫描端口总数：PortScan通常表现为大量的端口扫描行为；
  3. 平均正常包长与攻击包长的比例：由于PortScan的目的是探测目标主机的漏洞和弱点，以便进行后续的攻击或侦察，因此其包长普遍较短；
  4. 平均包间隔时间与正常链接的比例：PortScan表现为大量快速的扫描，因此其包间隔时间普遍较短；
  5. 链接平均持续时间：因PortScan仅以扫描端口为目的，故其链接持续时间通常较短。

通过以上指标可以将PortScan攻击有效的可视化。

3.4.2 DDoS可视化

根据前文中提到的DDoS监测方法，可以将以下信息进行可视化处理：

* 1. 攻击源IP及其端口：DDoS表现为大量的网络连接请求，因此该攻击可以检测到大量的攻击IP；
  2. 受攻击端口：DDoS以消耗目标设备的网络资源为目的，因此其通常会对固定的某个端口进行攻击，以确保目标的网络资源能被消耗殆尽；
  3. 攻击链接总数：为了消耗大量的网络资源，该攻击往往会产生大量网络链接以期消耗目标网络资源；
  4. 平均连接时间：DDoS通常保持长时间的连接，以此来占用目标的端口；
  5. 链接空闲与活跃时间比例：相比正常链接，DDoS的链接通常表现为极不活跃；
  6. 数据包信息：DDoS的数据包表现为长度高、速率低、间隔长的特点，因此将这些信息进行可视化并与正常链接对比可以很好的展示该类型的攻击。

通过以上指标可以将DDoS攻击有效的可视化。

3.4.3 其它类型攻击

在CICIDS2017数据集中，因为其它几类攻击的特征并不明显，因此这里对其以下几类信息进行可视化：

* 攻击IP及端口
* 被攻击端口
* 攻击链接数
* 攻击总流量
* 每分钟平均攻击速率

3.5本章小结

本章介绍了基于规则监测和机器学习的安全评估与可视化方法。针对CICIDS2017数据集中的PortScan和DDoS攻击，提出了基于统计预测的检测方法。

PortScan攻击主要针对网络中的主机和服务的端口进行大量的扫描和探测，以获取目标主机的开放端口和服务信息。DDoS攻击与其他网络攻击相比具有大规模、分布式和持久性的特点。通过结合CICIDS2017数据集中的流量特征，可以使用多个指标来判断流量是否为PortScan或DDoS攻击。

机器学习评估中，决策树是一种常用的分类算法。本文选用分类回归树（CART）作为决策树算法，用于流量分类任务。

针对PortScan和DDoS攻击的可视化方法，可以将相关指标进行可视化处理，以有效展示这些攻击类型。对于CICIDS2017数据集中的其他攻击类型，因其特征不明显，可以对攻击IP及端口、被攻击端口、攻击链接数、攻击总流量和每分钟平均攻击速率等信息进行可视化。

总结来说，本章重点介绍了基于统计预测和机器学习的安全评估与可视化方法，包括PortScan和DDoS攻击的检测和可视化，以及其他攻击类型的部分可视化信息。

# 系统设计与实现

4.1工作流程

系统设计主要分为数据预处理、模型训练、统计分析和入库可视化几个部分。

数据处理部分将CICIDS2017数据集进行合并、清洗、编码等操作，使其能够适用于后续模型训练以及统计分析。模型训练部分将处理好的数据读入，经过训练后生成模型文件并保存，用于后续模拟数据的预测。

由于DDoS、PortScan攻击的攻击特性较为明显，因此使用统计分析的方法。将二者数据单独取出，根据设定好的标准进行判别，为每条数据打上相应的攻击类型标签。最后是入库可视化部分，这里将前面已经分类好的文件依照其攻击类别写入数据库，并在可视化软件中进行展示。

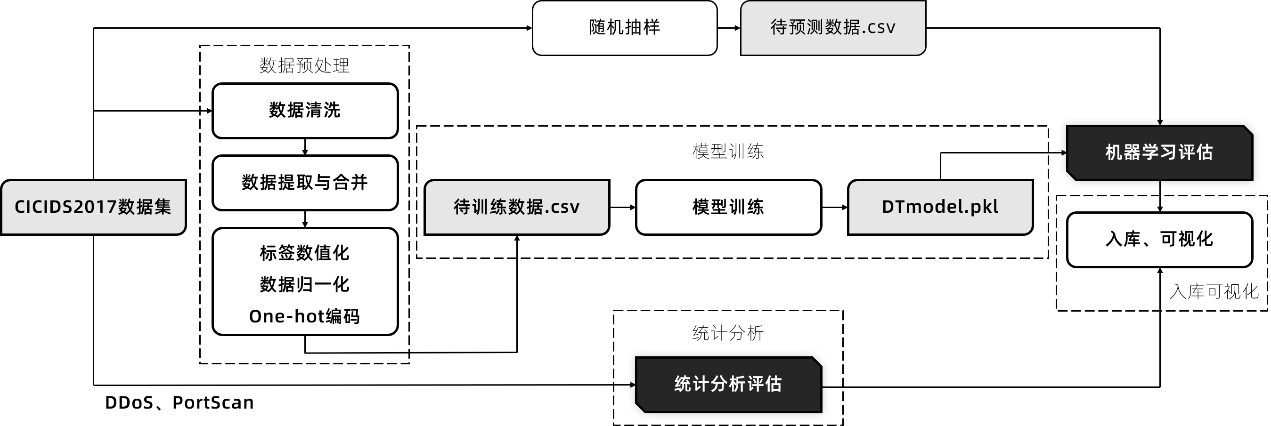


图 4–1 系统架构

4.2数据预处理

数据预处理是指对原始数据进行清洗、转换和整理的过程，以使数据适合于机器学习算法的训练和使用。数据预处理可以对数据进行有效的处理和转换，提高模型的性能和准确度。

4.2.1 数据清洗

机器学习的原始数据常常包含缺失值、异常值和噪声，数据清洗的目的在于纠正或清除数据中的错误信息，包括无效值、缺失值以及检测数据合理性，即替换、修正或删除脏数据。

本实验数据集中存在多处内容错误的数据，特别是Flow\_Bytes/s和Flow\_Packets/s这两列数据有一千多个“Infinity”和“NaN”的数据。然而，这些数据应该是数字形式的，这是明显的内容错误。

在对CICIDS2017数据集进行进一步处理之前，需要删除或替换具有NaN值和Infinity值的行。在本文中，由于CICIDS2017数据集中的NaN值和Infinity值相对较少，所以仅删除具有这些值的行。为此，使用numpy库中的isnull()和isinf()函数查找需要删除的行，并使用删除函数进行删除操作。

代码4-1 删除"Infinite"和"NaN"代码

|  |
| --- |
| def cleardata(file\_path, file\_name):  # 读取 csv 文件并计算总行数  df = pd.read\_csv(file\_path)  total\_rows = df.shape[0]  # 判断第14列和第15列是否存在缺失值和无穷值  row\_mask = df.apply(lambda row: pd.isnull(row[14]) or np.isinf(row[14]) or pd.isnull(row[15]) or np.isinf(row[15]), axis=1)  # 统计要删除的行数并删除特定行  rows\_to\_remove = row\_mask.sum()  df = df[~row\_mask]  # 统计最后一列标签类别及其数量  label\_counts = df.iloc[:, -1].value\_counts() |

由处理后的结果如下表可见，该数据集的各类标签数量极不平衡，这种情况下直接进行机器学习可能导致预测结果出现较大偏差[32]，因此本文只采用了“Friday-workinghours-Afternoon-DDoS.pcap\_ISCX.csv”、“Friday-workinghours-Afternoon-PortScan.pcap\_ISCX.csv”、“Tuesday-workinghours.pcap\_ISCX.csv”、“Wednesday-workinghours.pcap\_ISCX.csv”四个数据文件，并去除了Heartbleed攻击类型（仅11条数据）。将以上得到的数据文件进行合并，并统计各个攻击类别的标签。结果见下表：

表4-1 total.csv中各个攻击类别标签及行数

| **标签** | **行数** | **标签** | **行数** |
| --- | --- | --- | --- |
| 总行数 | 1648858 | DoS goldeneye | 10293 |
| BENIGN | 1096474 | FTP-Patator | 7935 |
| DoS Hulk | 230124 | SSH-Patator | 5897 |
| PortScan | 158804 | DoS slowloris | 5796 |
| DDoS | 128025 | DoS Slowhttptest | 5499 |

其中BENIGN和DoS Hulk两种类型的数量依然过大，因此使用numpy中的random.shuffle()函数采用随机抽样的方法各自去除一部分数据。

代码4-2 去除部分数据

|  |
| --- |
| # 删除 'dos Hulk' 类别中的随机 200000 个样本  dos\_hulk\_indices = df[df.iloc[:, -1] == 'dos hulk'].index.to\_numpy()  np.random.shuffle(dos\_hulk\_indices)  dos\_hulk\_indices\_to\_remove = dos\_hulk\_indices[:200000]  df = df.drop(dos\_hulk\_indices\_to\_remove)  # 删除 'benign' 类别中的随机 1060000 个样本  benign\_indices = df[df.iloc[:, -1] == 'benign'].index.to\_numpy()  np.random.shuffle(benign\_indices)  benign\_indices\_to\_remove = benign\_indices[:1060000]  df = df.drop(benign\_indices\_to\_remove) |

最终得到用于训练的攻击类型如下：

表4-2 total\_sub.csv中各个攻击类别标签及占比

| **标签** | **总行数** | **占比** |
| --- | --- | --- |
| BENIGN | 36474 | 35.8% |
| DoS Hulk | 30124 | 29.5% |
| DoS goldeneye | 10293 | 10.1% |
| FTP-Patator | 7935 | 7.8% |
| SSH-Patator | 5897 | 5.8% |
| DoS slowloris | 5796 | 5.7% |
| DoS Slowhttptest | 5499 | 5.4% |

4.2.2 标签数值化

在经过上述处理的CICIDS2017数据集中，包含了7种类型，其中包括BENIGN类和6种攻击类型，这些类型的名称在数据集中以字符串的形式进行存储。由于机器学习算法无法直接对字符串类型的数据进行训练，因此在进行训练之前，需要将这些类型标签转化为数字标签。本文中使用pandas中的factorize()对这7种类型名进行替换。

代码4-3 标签数值化

|  |
| --- |
| # 加载数据  data = pd.read\_csv(data\_path, header=none)  # 将最后一列转换为数值型  label\_mapping = pd.factorize(data[78])  data[78] = label\_mapping[0] |

表4-3 数值化后的各个标签

| **数据类型** | **数值标签** |
| --- | --- |
| BENIGN | 0 |
| DoS slowloris | 1 |
| DoS Slowhttptest | 2 |
| DoS Hulk | 3 |
| DoS goldeneye | 4 |
| FTP-Patator | 5 |
| SSH-Patator | 6 |

4.2.3 特征选择

机器学习中特征选择的目的是从原始特征集中选择最相关和最具有信息量的特征，以提高模型性能和效率。特征选择是机器学习中的关键步骤，它有助于减少特征空间的维度，从而降低计算成本，并提高模型的泛化能力[33]。

特征选择的主要目标包括：

* 1. 提高预测性能：通过选择最相关的特征，可以减少特征间的冗余信息，使模型能够更好地捕捉数据中的关键特征，从而提高预测性能；
  2. 减少过拟合：过多的特征可能导致模型过于复杂，容易过拟合训练数据，而特征选择可以剔除无关或冗余的特征，减少模型的复杂性，降低过拟合的风险；
  3. 加速训练过程：特征选择可以减少特征空间的维度，从而减少计算和存储的开销，加快模型的训练过程和预测速度；
  4. 改善模型解释性：选择最相关的特征可以帮助我们理解数据中的重要因素和关联关系，提供更好的可解释性和洞察力。

本文采用递归特征消除（Recursive Feature Elimination, RFE）的方法进行特征排序，并通过随机森林分类器对特征数进行交叉验证选择。

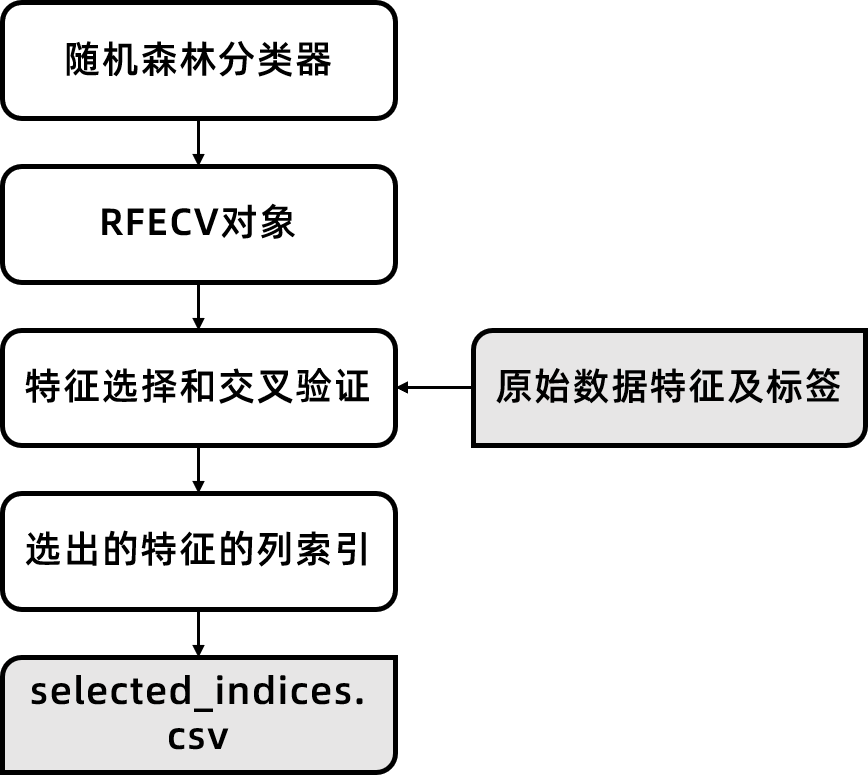


图 4–2 特征选择流程

首先将对原始数据进行切片，分离出特征和标签，随后送入featureSelect()进行特征选择。在featureSelect()中创建随机森林分类器作为估计函数，并创建RFECV对象进行特征选择和交叉验证，最后利用getSelectedFeatureIndices()导出列索引，与其标签一并返回。

代码4-4 特征选择并导出保存

|  |
| --- |
| # 对原始数据进行切片，分离出特征和标签  features = data\_sample.iloc[:, 0:78]  labels = data\_sample.iloc[:, 78]  # 对原始特征进行选择  selected\_features, selected\_indices = featureSelect(features, labels)      def featureSelect(features, labels):  # 创建随机森林分类器作为估计函数  estimator = RandomForestClassifier()  # 创建RFECV对象，设置最少选择特征数为36  rfecv = RFECV(estimator=estimator, min\_features\_to\_select=36, cv=KFold(n\_splits=2))  # 进行特征选择和交叉验证  rfecv.fit(features, labels)  print("选出的特征数: ", rfecv.n\_features\_)  print("特征重要性排序:\n", rfecv.ranking\_)  # 获取选出的特征的列索引  selected\_indices = getSelectedFeatureIndices(rfecv.ranking\_)  # 提取选出的特征  selected\_features = features.iloc[:, selected\_indices]  return selected\_features, selected\_indices  def getSelectedFeatureIndices(ranking):  selected\_indices = [i for i, rank in enumerate(ranking) if rank == 1]  print("选出的特征列索引:\n", selected\_indices)  return selected\_indices |

下表列出了递归特征消除算法得出的第1-78个特征（由上至下，从左到右）的重要性排序。这是在RFECV中挑选出指定特征的重要性排序。本文将选出来的最优的65个特征用于后续实验的学习。

表4-4 标签重要性排序

|  |
| --- |
| 1 1 1 1 1 1 1 1 1 1 1 1 1  1 1 1 1 1 1 1 1 1 1 1 1 1  1 1 1 1 1 10 8 14 1 1 1 1 1  1 1 1 1 1 1 7 1 1 1 11 6 1  1 1 1 1 9 12 5 4 13 3 1 1 1  1 1 1 1 1 1 2 1 1 1 1 1 1 |

4.2.4 数据标准化

数据标准化（Standardization）也称为z-score标准化，是机器学习中常用的数据预处理技术，用于将原始数据转换为更适合模型训练的形式，目的是将不同特征之间的数值范围进行统一，消除特征之间的量纲差异，以便更好地适应机器学习算法。

数据标准化使用均值和标准差进行线性变换，将原始数据转换为均值为0、标准差为1的分布。具体做法是对每个特征进行减去均值，再除以标准差。这样做可以使得数据分布更接近标准正态分布，有助于提高模型的稳定性和收敛速度。该方法适用于特征的分布近似正态分布的情况。

本文中使用pandas中的preprocessing.scale()对标签数据进行标准化，用于后续模型训练。

代码4-5 特征数据标准化

|  |
| --- |
| # 特征数据标准化  features\_normalized = pd.dataframe(preprocessing.scale(selected\_features)) |

4.2.5 One-hot编码

采集的数据中如流量标签部分不是连续型数据，而是离散型数据。之前的工作中已将标签数值化，而此时数据并不能直接用在模型中，因为分类器往往默认数据是连续的，并且是有顺序的。但按照标签的含义，该转换数字并不是有序的，而是随机分配的，数值的大小也并无实际意义。

采用One-hot编码（One-hot Encoding）可以解决这个问题。One-hot编码是一种常用的数据编码方法，用于将分类变量表示为二进制向量。在One-hot编码中，对于具有N个不同类别的特征，将其转换为一个长度为N的二进制向量，其中只有一个元素为1（表示当前类别），其他元素均为0。也可以理解为对于每一个特征，如果它有ｍ个可能值，那么经过One-hot编码后，就变成了ｍ个二元特征。并且这些特征互斥，每次只有一个特征被激活。

例如，假设有一个特征"颜色"，可能的取值有"红色"、"绿色"和"蓝色"。使用One-hot编码后，可以将"红色"表示为[1,0,0]，将"绿色"表示为[0,1,0]，将"蓝色"表示为[0,0,1]。每个类别都被编码为一个唯一的二进制向量，以便在机器学习算法中能够处理分类变量。

One-hot编码能够有效地表示分类变量，避免了不同类别之间的大小关系对模型的影响。编码后既解决了数据属性问题，又将实验数据集中的7个标签，扩展成七维的稀疏标签变量。

本文中首先使用labels.values将标签数据转换为一个numpy数组，其次使用flatten()函数将多维数组压平为一维数组，目的是简化数据处理过程，使得数据更易于使用和传递。再使用pandas中get\_dummies()，实现了对数据标签的One-hot编码。

代码4-6 标签数据One-hot编码

|  |
| --- |
| # 将多维的标签转为一维的数组  labels\_array = labels.values.flatten()  # onhot 编码  labels\_encoded = pd.get\_dummies(labels\_array) |

将准备好的数据导出为csv，以备后续模型训练使用。



图 4–3 预处理完成的数据

4.3模型训练

读入上述准备好的数据文件，实例化一个DecisiontreeClassifier并设置以下参数：

表4-5 DecisiontreeClassifier模型参数设置

|  |  |
| --- | --- |
| **参数** | **数值** |
| criterion | entropy |
| max\_depth | 12 |
| min\_samples\_leaf | 1 |
| splitter | best |

选取entropy（信息熵）作为criterion划分准则。在决策树中，熵的值越高，表示数据集的不确定性越大，纯度越低；而熵的值越低，表示数据集的纯度越高，不确定性越小。entropy划分准则在处理多分类问题时比较常用，尤其适用于处理具有不均衡类别分布的数据。它能够有效地对各个类别的不确定性进行量化，并在决策树的构建中寻找最佳的划分方式。

max\_depth=12指定了决策树最大深度，避免过拟合并控制决策树的复杂度。

代码4-7 决策树模型训练

|  |
| --- |
| clf = decisiontreeclassifier(criterion='entropy', max\_depth=12, min\_samples\_leaf=1, splitter="best")  clf.fit(x\_train, y\_train)  y\_pred = clf.predict(x\_test)  accuracy = accuracy\_score(y\_test, y\_pred)  joblib.dump(clf, model\_path + "\dtmodel.pkl") |

模型精度为0.9977，将模型保存为dtmodel.pkl文件。

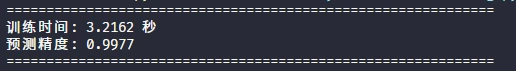


图 4–4 模型训练结果

4.4机器学习检测

4.4.1 待预测数据生成

从CICIDS2017原始数据集中随机抽取100000行数据用于后续预测，其中攻击类型仅包含七种模型学习过的攻击类型。

代码4-8 生成待预测数据

|  |
| --- |
| # 随机抽取指定行数的数据  sampled\_data = data.sample(n=preamount, random\_state=42)  # 将抽样结果保存到新的csv文件  sampled\_data.to\_csv(output\_file, index=false, header=false) |

4.4.2 模型数据预测

该部分首先读取待预测数据、选取特征列表、模型文件。其次，针对预测数据中的每一行进行如下处理：

* 1. 丢弃0, 1, 2, 3, 5, 6列，这一部分的数据不适用于机器学习，因此模型的训练数据中也不包含该部分；
  2. 根据上文生成的选取特征列表，选择需要进行预测的特征列，送入模型预测；
  3. 得到One-Hot编码形式的标签结果，将此结果转换为原始攻击标签类型字符串；
  4. 将原始数据行和预测得到的标签字符串组合。

最后将所有预测结果统一输出为predicted.csv，用作后续入库可视化。

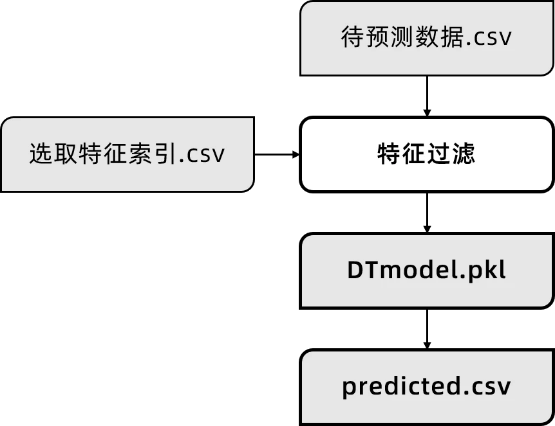


图 4–5 模型学习评估流程

代码4-9 模型学习评估

|  |
| --- |
| def predict\_byrow(file\_path):  # 加载模型  data = pd.read\_csv(file\_path, header=none)  model = joblib.load(model\_path)  predicted\_data = []    for index, data\_row in data.iterrows():  row = data\_row.drop([0, 1, 2, 3, 5, 6]).reset\_index(drop=true)  features = row[selected\_indices] # 提取选中的特征列  label\_onehot = model.predict([features])[0] # 进行标签预测（返回的是one-hot编码）  label = label\_mapping\_inverse[label\_onehot.argmax()] # 将one-hot编码转换为原始标签  data\_row = data\_row.tolist() + [label]  predicted\_data.append(data\_row) |

4.5规则匹配检测

根据前文的统计分析评估方法，首先对于DDoS以及PortScan攻击每个需要判断的指标，在整个数据集中求出其正常值或范围，然后针对预测数据的每一行进行判断，若该行数据偏离正常值较远，则判断为异常流量，打上相应标签后写入预测结果文件，进行入库可视化。

代码4-10 规则分析判断DDoS攻击

|  |
| --- |
| for index, row in data.iterrows():  if (row['total fwd packets'] > threshold\_fwd\_packets) and \  (row['total backward packets'] > threshold\_bwd\_packets) and \  (row['total length of fwd packets'] > threshold\_fwd\_length) and \  (row['total length of bwd packets'] > threshold\_bwd\_length) and \  (row['flow duration'] > threshold\_duration) and \  (row['destination port'] in suspicious\_ports) and \  (row['flow iat mean'] > threshold\_mean) and \  (row['flow iat std'] > threshold\_std):  ddos\_label.append("ddos")  else:  ddos\_label.append("benign")  data\_row = data\_row.tolist() + [label]  predicted\_data.append(data\_row) |

4.6设备实时信息采集

修改位于/etc/telegraf/telegraf.conf中的Telegraf默认配置文件，插件配置信息如下：

* net、netstat、cpu、mem、disk：设置为默认配置，收集设备的网络和CPU、磁盘等信息；
* dns\_query：设置 domains = [

"www.google.com",

"www.baidu.com",

"www.bilibili.com",

"www.nwpu.edu.cn",

"www.qq.com",

"www.douyin.com",

"cn.aliyun.com",

"github.com",

]

用于监测常用网站的DNS查询时间情况；

* net\_response：网站配置如上，用于监测网站的连通性；
* influxdb：配置数据库名及用户密码，用于收集数据的写入。

保存并重启Telegraf，此时即可收集相关资源信息。

4.7数据入库

该部分中，由于数据量较大以及机器性能限制，首先将预测好的数据拆分为数个文件，方便后续入库。其次将数据依次读入，根据其预测标签分类送入不同的measurement表。

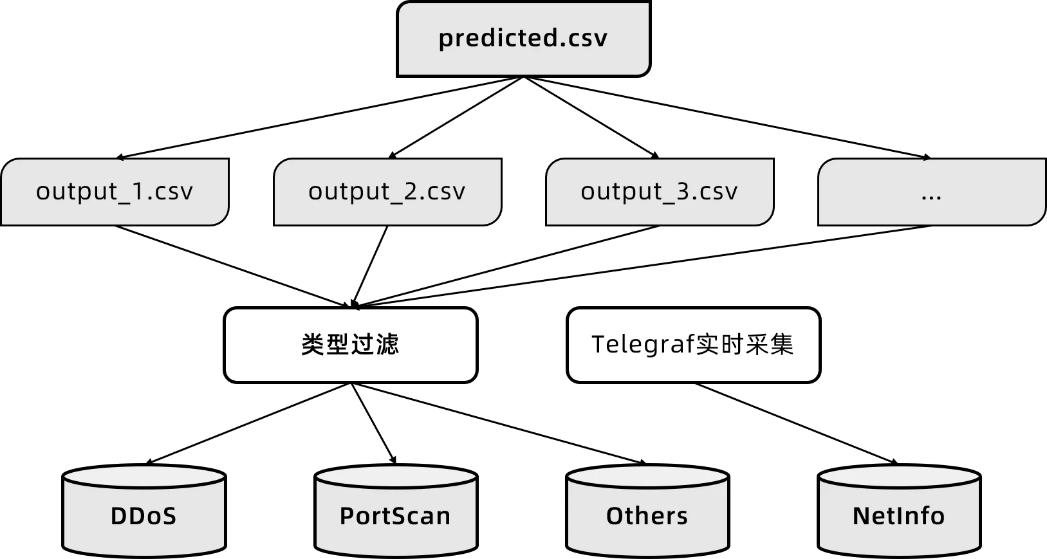


图 4–6 数据入库流程

InfluxDB中共分为四个数据库，分别存储DDoS攻击数据、PortScan攻击数据、其它类别攻击数据以及设备实时性能。每个数据库中根据其攻击类别分为不同的measurement表，用于Grafana进行查询可视化。

4.8测试与结果

4.8.1 实验环境

本文实验采用的是i5-10210U处理器、内存为16G的笔记本电脑。物理机操作系统为Windows11，虚拟机为Centos7.9：，虚拟机使用的平台为：vmware 16.2.5。其它开发软件版本如下：

表4-6 实验所用开发软件版本

| **平台** | **版本** |
| --- | --- |
| Telegraf | 1.26.2 |
| InfluxDB (centos) | 1.8.10 |
| Grafana | 9.1.2 |
| Pandas | 1.3.5 |
| Numpy | 1.21.6 |
| Scikit-learn | 1.0.2 |
| InfluxDB (python) | 5.3.1 |

4.8.2 数据库情况

利用/usr/bin/influx命令进入InfluxDB查看数据情况，其中包含四个前文创建的数据库，可以看到在netinfo中包含已收集的设备信息：

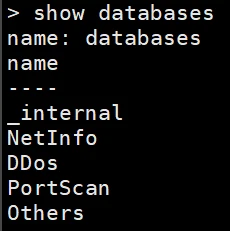
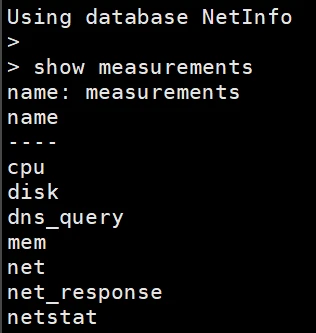
 

图 4–7 数据库情况 图 4–8 netinfo数据库表

DDoS库中则包含83265条攻击数据：

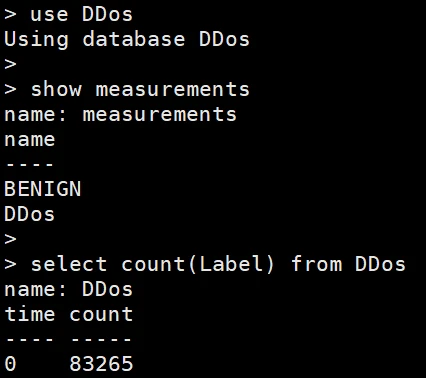


图 4–9 netinfo数据库表

表4-7 各数据库表攻击链接数据量

| **数据库（表）** | **数据量** |
| --- | --- |
| DDoS | 83265 |
| PortScan | 42175 |
| DoS\_goldeneye | 8149 |
| DoS\_Hulk | 28725 |
| DoS\_Slowhttptest | 5156 |
| DoS\_slowloris | 5764 |
| FTP\_Patator | 4582 |
| SSH\_Patator | 3576 |

4.8.3 结果可视化

通过浏览器访问http://192.168.10.100:3000/，进入Grafana配置页面。首先将InfluxDB中的数据库配置为数据源，然后在Dashboard面板中可以添加相应的可视化面板。

根据前文中提到的可视化指标，对各个攻击类型及设备信息进行可视化配置，可根据需求选择Time series、Stat、Gauge、Table、Pie chart等形式进行可视化：

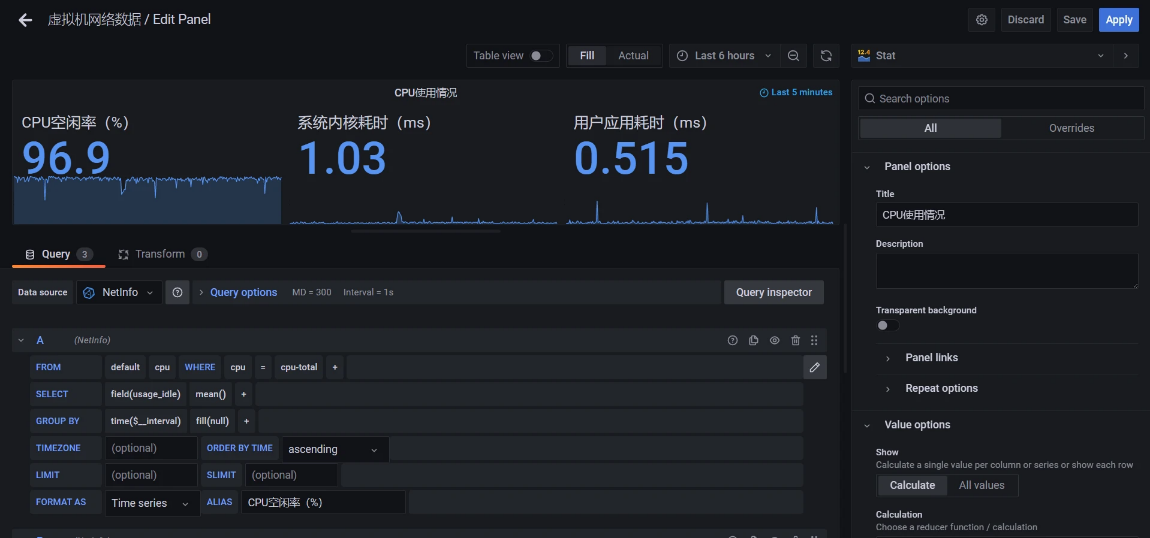


图 4–10 可视化配置界面

最终结果展示如下：

**网络攻击信息：**

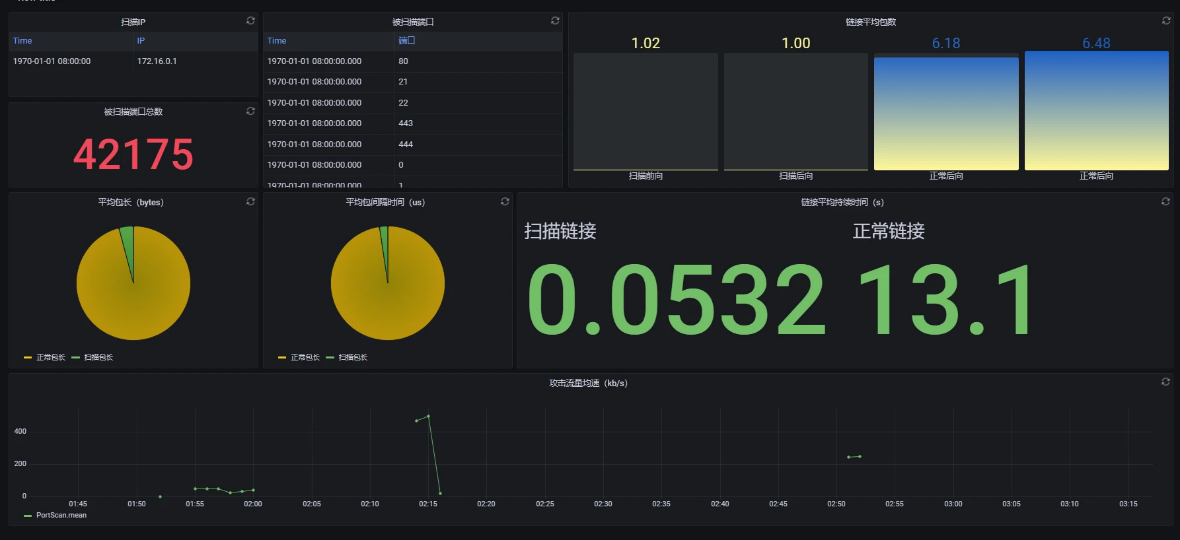


图 4–11 PortScan结果可视化



图 4–12 DDoS结果可视化

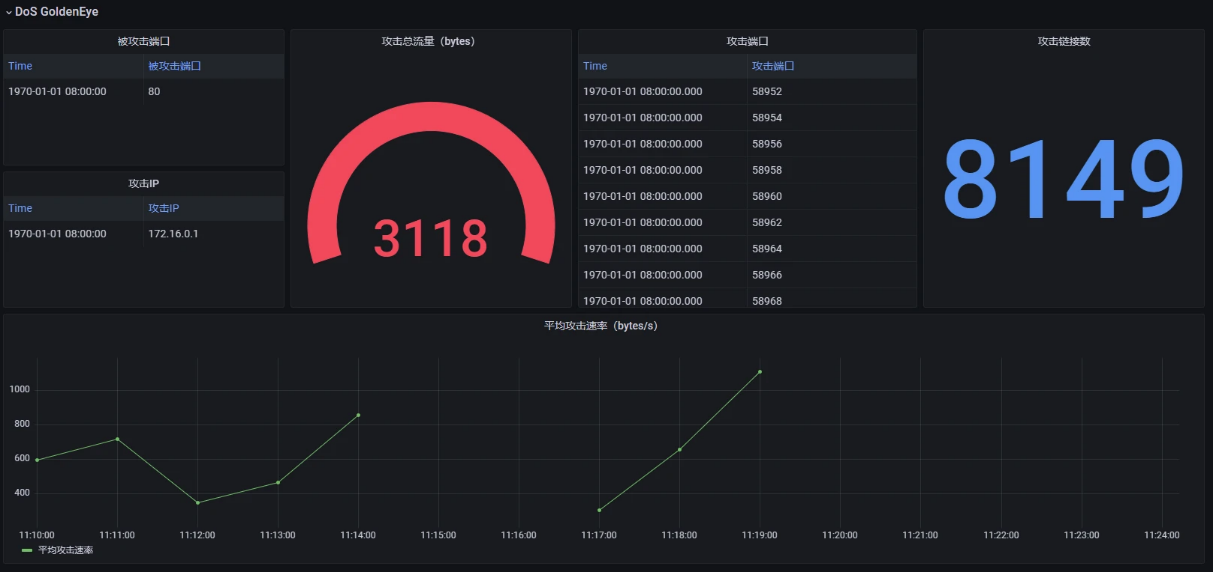


图 4–13 DoS\_GoldenEye

**设备状态信息：**

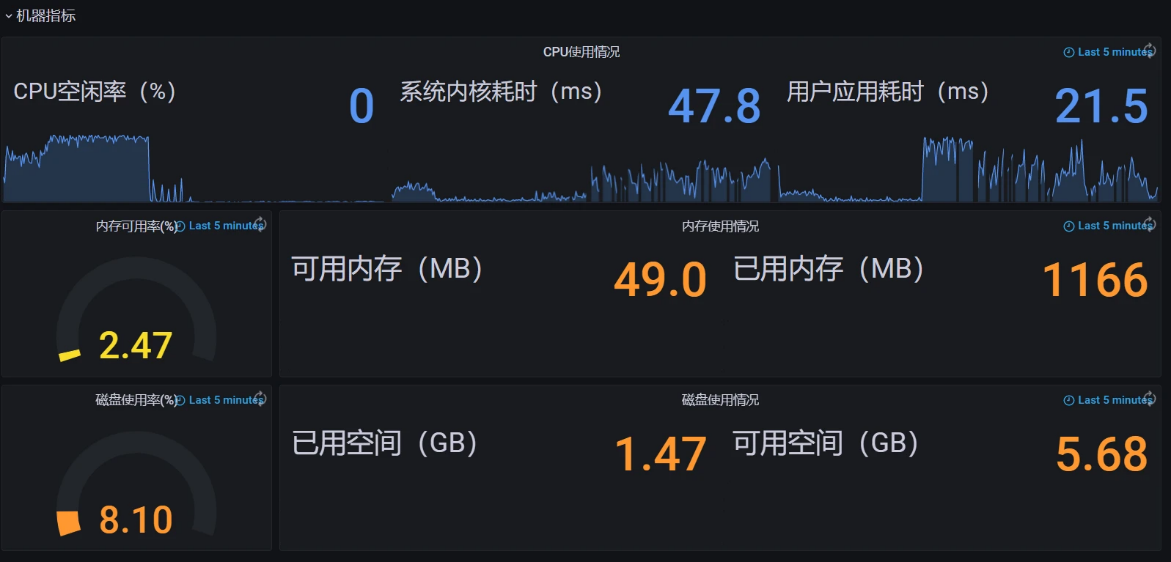


图 4–14 设备指标



图 4–15 站点响应

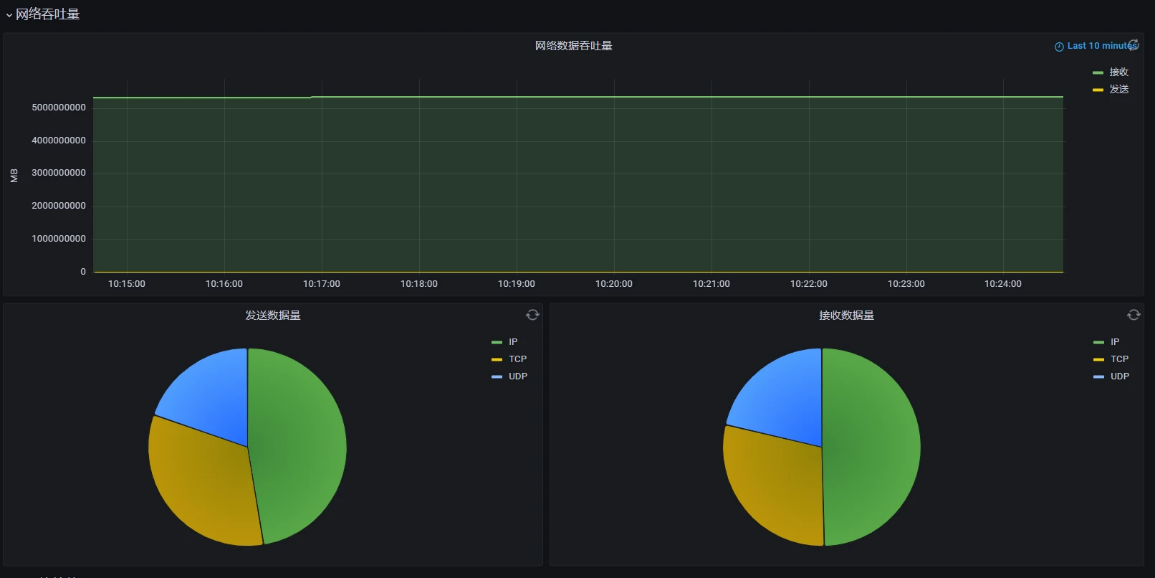


图 4–16 网络吞吐量



图 4–17 TCP连接数

4.8.4 实时数据发送测试

从原始数据中抽取约10000条数据进行测试，在reader.py中设置每次读取200条数据，间隔0.01秒，在grafana面板中可得结果如下：

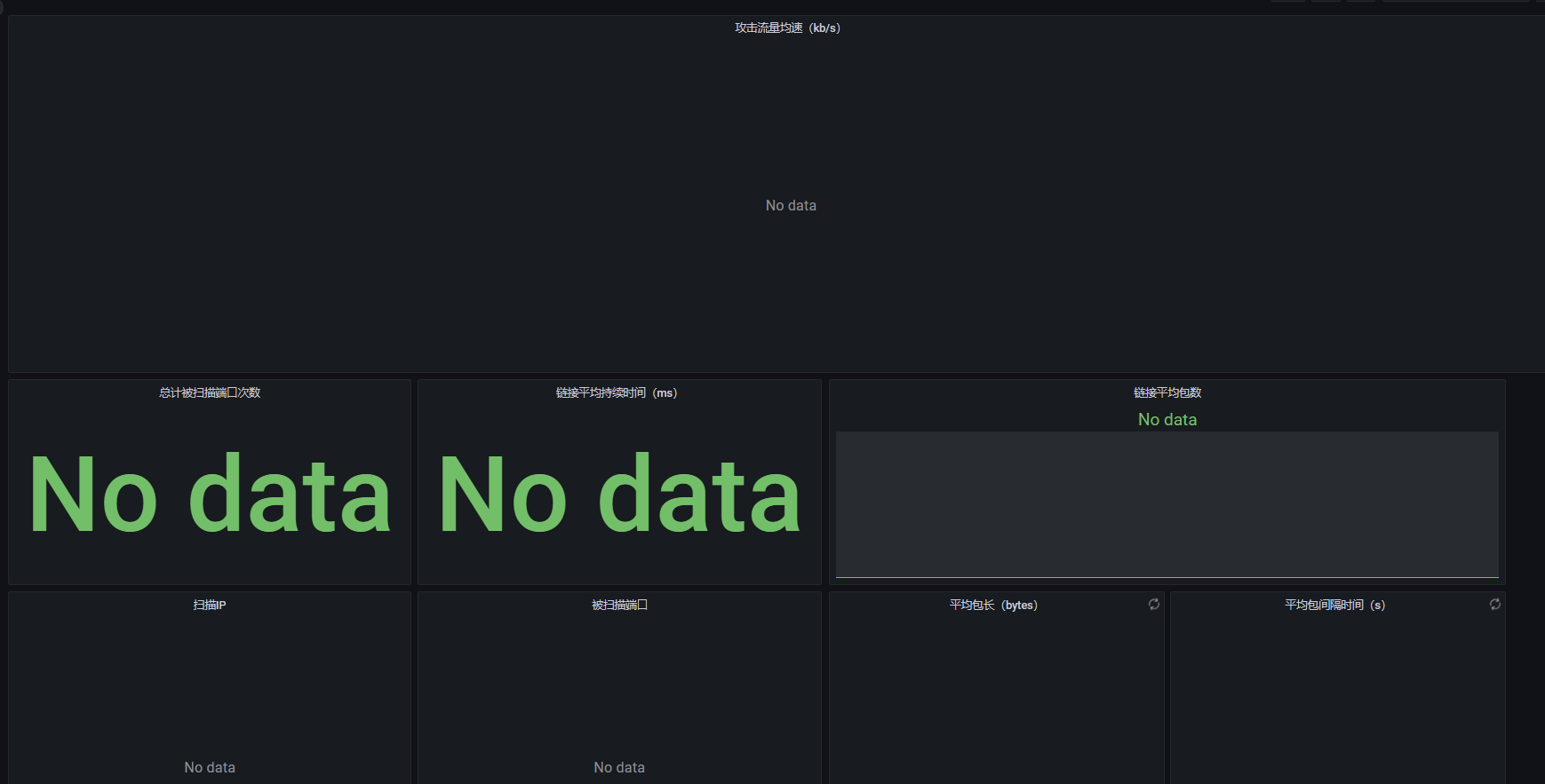


图 4–18 攻击数据发送前可视化面板

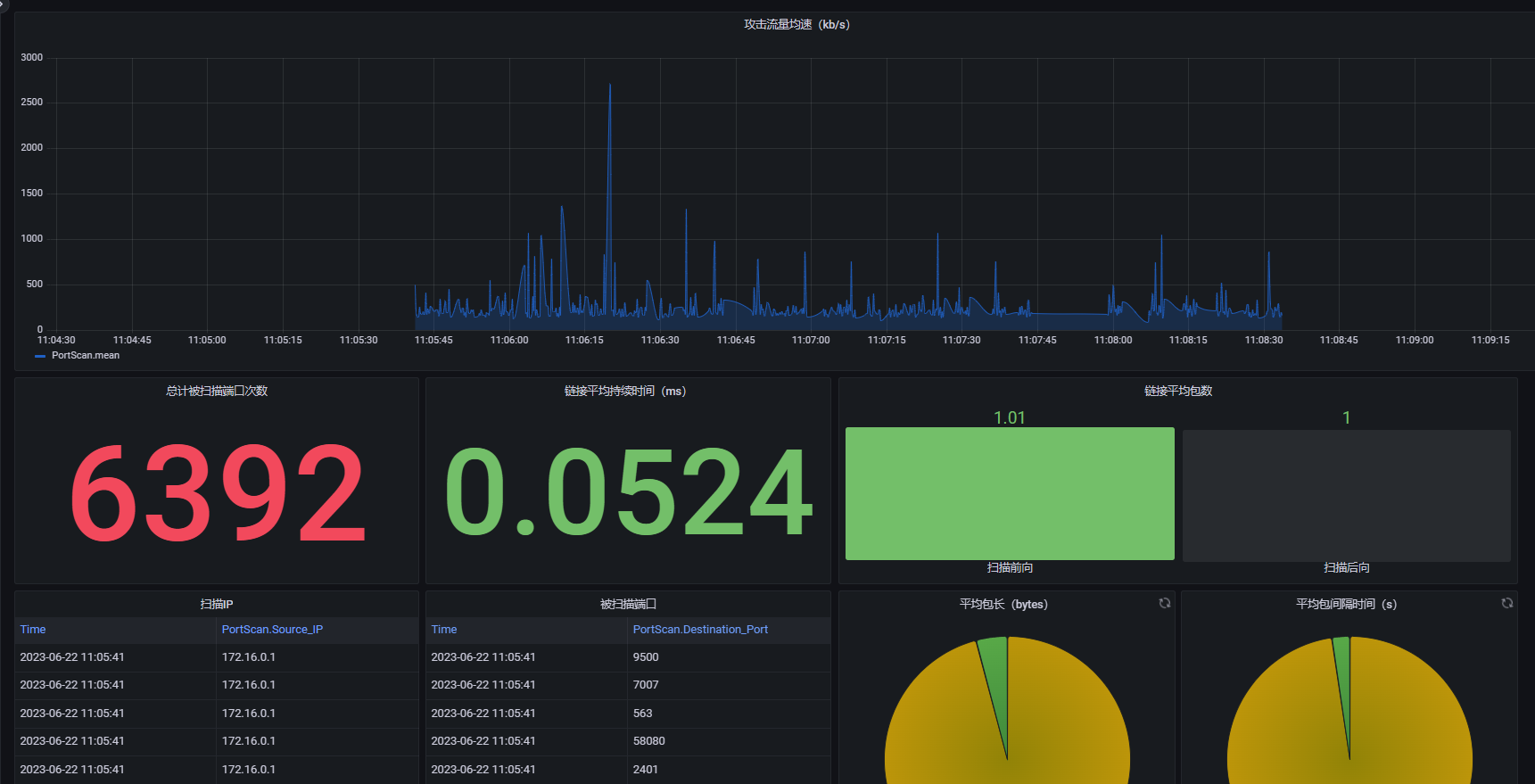


图 4–19 攻击数据发送后可视化面板

可以看到graafana可以实时的接收到已经检测入库的攻击数据。

4.8.5 准确性评判及分析

将系统评估得出的攻击类型与原始类型进行对比，得出系统的评估准确性测试如下表。可以看到在所有的攻击类型中，各个类型的准确率基本都在百分之八十左右，其中DDoS和PortScan两类使用规则匹配的攻击检测准确率较低，而其它的机器学习检测方式准确率相对较高。推测这种结果的可能原因是规则匹配的方式检测手段单一，无法全面的检测出每一个攻击流量，并且其适应能力差，对于稍有不同的攻击流量则无法正确识别，因此导致其准确率较低。

表4-8 各攻击类型评估准确性测试

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **类型** | **总行数** | **第一次** | **第二次** | **第三次** | **平均准确率** |
| DDoS | 12728 | 9866 | 9735 | 9941 | 77.4% |
| PortScan | 15732 | 11428 | 11932 | 12754 | 76.5% |
| DoS Hulk | 30124 | 24958 | 24966 | 24799 | 82.7% |
| DoS GoldenEye | 10293 | 9011 | 9126 | 8912 | 87.6% |
| DoS slowloris | 5796 | 4829 | 4709 | 4621 | 81.4% |
| DoS Slowhttptest | 5499 | 4631 | 4721 | 4864 | 86.2% |
| FTP-Patator | 7935 | 7036 | 7019 | 6923 | 88.1% |
| SSH-Patator | 5879 | 4976 | 4721 | 4832 | 82.4% |

# 总结与展望

5.1已完成工作

本文工作前期首先进行了广泛的资料文献查询，对网络安全评估与可视化进行初步了解。首先，经过多方对比，选取CICIDS2017数据集作为数据源，这是一个广泛使用的网络入侵检测数据集，用于评估和研究入侵检测系统的性能。其次，系统开发语言选择了Python，它拥有丰富的机器学习库以及简洁而高效的语法，使得开发者能够更加高效地进行机器学习任务。

系统开发过程中，数据集的处理是一大难题。CICIDS2017拥有极为庞大的数据量，这为机器学习提供了丰富的学习材料时也使前期数据处理面临挑战。例如在进行数据入库测试过程中，时常出现数据库连接超时的问题。为解决该问题，本文首先将其分割为数个较小的CSV文件，然后利用sleep函数控制其发送时间间隔，确保数据入库的完整性。

其次是模型训练阶段，通过对比不同的训练方法，发现决策树相较于其它的方法，在拥有较快的训练速度的同时还能保持相当的准确率，因此在训练阶段使用决策树进行攻击类型预测。

同时，由于数据量较大，以及为了保持各个阶段的独立性以及测试的方便性，系统将每个阶段的数据结果都独立保存，各个阶段的任务执行都不会受到其它阶段的影响。

最后，系统采用Telegraf + Influx DB + Grafana的方式搭建数据可视化平台。这是一种目前较为成熟的方式，各自都拥有比较丰富的生态和极佳的实用性。系统将所有预测数据导入InfluxDB中，同时利用Telegraf 采集设备的实时信息，最终利用Grafana实现数据的可视化。

综上，本系统是一个结合了机器学习以及规则匹配的网络安全评估可视化系统，通过一系列的方法和手段实现网络流量的性质判断，最终将结果可视化的呈现出来。

5.2未来展望

目前本系统是基于固定数据集的预测系统，针对网络世界的真实流量信息的预测还没有实现。另外，基于规则的预测方法还较为简单，无法应对真实的复杂数据情况，而采用决策树的机器学习方法也有较大的局限性，比如容易过拟合导致在新数据上的泛化性能下降，同时决策树独立地对每个特征进行分割，可能会忽略特征之间的相关性。

针对以上问题，后续将采用更为成熟的技术方案，实现实时网络流量的安全评估预警。同时也可以采用深度学习的方式，如神经网络对数据进行学习，以确保对新数据和真实数据的预测准确性。

# 参考文献

* 1. 国家互联网应急中心. 2020年中国互联网网络安全报告[R].2021.http://www.cac.gov.cn/2021-07/21/c\_1628454189500041.htm
  2. 赵颖,樊晓平,周芳芳等.网络安全数据可视化综述[J].计算机辅助设计与图形学学报,2014,26(05):687-697.
  3. 吕良福,张加万,孙济洲等.网络安全可视化研究综述[J].计算机应用,2008, 216(08):1924-1927.
  4. 袁斌,邹德清,金海.网络安全可视化综述[J].信息安全学报,2016,1(03):10-20. DOI:10.19363/j.cnki.cn10-1380/tn.2016.03.002.
  5. Buczak, Anna L, et al. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection[J]. Communications Surveys & Tutorials, 2017, 18(2): 1153-1176.
  6. Farnaaz N , Jabbar M A . Random Forest Modeling for Network Intrusion Detection System[J]. Procedia Computer Science, 2016, 89:213-217.
  7. Wang, Huiwen Gu, Jie Wang, Shanshan.An effective intrusion detection framework based on SVM with feature augmentation[J].Knowledge-based systems, 2017, 136:130-139.
  8. Bhattacharjee PS, Fujail AKM, Begum SA. A Comparison of Intrusion Detection by K-Means and Fuzzy C-Means Clustering Algorithm Over the NSL-KDD Dataset[A]. 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). IEEE, 2017.
  9. Akashdeep, Manzoor I, Kumar N. A Feature Reduced Intrusion Detection System Using ANN Classifier[J]. Expert Systems with Applications, 2017, 88:249-257.
  10. FORTIER S C,SHOMBERTLA.Network profiling and data visual-ization[A]. Proceedings of the2000IEEE Workshop on Informa-tion Assurance and Security.West Point,NY:IEEE,2000:166-169.
  11. LAKKARAJUK,YURCIKW,LEE AJ.NVisionIP:netflowvisu-alizations of system state for security situational awareness[A]. ACMWorkshop Visualization and Data Mining for Computer Secur-ity.New York:ACMpress,2004:65-72.
  12. MALECOTE L, KOHARA M, HORI Y.Interactively combining 2D and 3D visualization for network traffic monitoring[A]. Visualization for Computer Security.NewYork:ACMPress,2006:123-127.
  13. McPHERSON J,MA K L,KRYSTOSK P.Portvis:a tool for port-based detection of security events. [2007-08-16]. <http://www.cs.ucdavis.edu/~ma/papers/portvis.pdf>.
  14. KOIKE H, OHNO K.SnortView: Visualization systemof snort logs[J].Visualization and Data Mining for Computer Security,2004:143-147.
  15. 甘刚.网络攻击与防御[M].清华大学出版社,2008．
  16. 吴婷,轻量级网页漏洞扫描工具的设计与实现[J]．电子设计工程，2019(12).
  17. 刘欣然.网络攻击分类技术综述[J].通信学报,2004 (07):30-36.
  18. Hong K., Y. Kim, H. Choi, J. Park. SDN-Assisted Slow HTTP DoS Attack Defense Method[J]. Communications Letters,2018,22(4): 688-691.
  19. B Danczul, J Fuß, S Gradinger, B Greslehner, et. Cuteforce Analyzer: A Distributed BruteForce Attack on PDF Encryption with GPUs and FPGAs, 2013 International Conference on Availability, Reliability and Security[J], 2013:720-725, doi: 10.1109/ARES.2013.94.
  20. Lai J, Wu S Chen, C Wu, C Yang. Designing a Taxonomy of Web Attacks [A]. Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology.
  21. Vormayr, G, T Zseby, J Fabin. Botnet Communication Patterns. IEEE Communications Surveys & Tutorials,2017,19(4): 2768-2796.
  22. 任日鹏. 信息收集在渗透攻击中的应用研究[J].电子测试, 2019,06: 62-63.
  23. Wheeler, D A. Preventing Heartbleed[J]. Computer, 2014,47(8): 80-83.
  24. 邢成.基于网络流量的异常检测算法研究[D].哈尔滨:哈尔滨工程大学,2020.DOI:10.27060/d.cnki.ghbcu.2020.001013.
  25. 康晓宁.分布式高速网络入侵防御系统研宄与试验性实现[D].北京:清华大学,2004.
  26. 许聪源.基于深度学习的网络入侵检测方法研究[D]. 浙江:浙江大学,2019.DOI:10.27461/d.cnki.gzjdx.2019.000045.
  27. Y X Meng. The Practice on Using Machine Learning for Network Anomaly Intrusion Detection [C]. International Conference on Machine Learning and Cybernetics, 2011: 576-581.
  28. S Sarvari, Z Muda, I Ahmad. GA and SVM Algorithms for Selection of Hybrid Feature in Intrusion Detection Systems [J]. Cyberspace Secur, 2015, 10:265.
  29. N B Aissa, M Guerroumi. A Genetic Clustering Technique for Anomaly-based Intrusion Detection Systems [C]. International Conference on Software Engineering, Artifacial Intelligence, 2015:1-6.
  30. Iman Sharafaldin, Arash Habibi Lashkari. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization [C]. 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, 2018.
  31. 郭楚栩,施勇,薛质.基于机器学习的端口扫描入侵检测 [J].通信技术,2020,53(02):421-426.
  32. 蓝亚之舟. CIC-IDS2017数据集训练和测试. 2021-03-20. <https://blog.csdn.net/yuangan1529/article/details/115024175>
  33. 卢琼. 基于深度学习的网络攻击检测技术的研究[D].北京:华北电力大学(北京),2020.DOI:10.27140/d.cnki.ghbbu.2020.001347.

# 致 谢

我即将完成本科毕业设计，也将告别西北工业大学，这四年的学习生涯让我充实而愉快。这里的严谨学风和美丽校园环境让我难以忘怀。回想起这段时光，我心中充满了对老师们耐心指导和同学们朝夕相伴的感激之情。我衷心地感谢所有帮助过我的老师和同学们，感谢他们对我的帮助和影响，让我能够克服困难并受益终身。

首先，我要衷心感谢我的导师潘炜教授。在毕业设计和科研论文写作过程中，潘炜老师给予了我巨大的帮助和不断的教诲。

我还要感谢那些为我提供参考文献的学者们，感谢他们为我提供了丰富的理论支持，使我的论文写作有了可依赖的依据。

我也要感谢我的家人和朋友们，尤其是我的父母。是你们在我大学四年生活中给予了我最大的支持和帮助。我们紧密相连，共同迈向更美好的未来。

在即将毕业之际，我内心充满了感激之情，真诚地感谢所有在西北工业大学陪伴我成长的老师和朋友们！

最后，我衷心感谢评阅老师的细心评阅。

# 毕业设计小结

回顾我大学四年的生活，最令我有成就感的时刻是进行毕业设计的日子。起初，我以为毕业设计只是一个类似于大作业的任务。然而，在完成毕业设计的过程中，我发现它不仅仅是一个作业，更是一个自我实现的项目。完成大作业只需要满足课程要求，而在毕业设计中，我时刻思考着如何采用更好的方法来实现更好的效果和更高的效率；我考虑着是否可以通过更简单直接的方式完成某个功能。每当我有新的想法时，我都会主动去尝试实现它，而每当成功地实现了一个模块中的新功能，我都会感到极大的成就感。

我的毕业设计课题是网络安全评估可视化。最开始，我将研究重点放在了可视化上而忽略了系统中最核心的评估部分，但经过老师指点后，我及时调整了研究思路，重点研究流量的类型评估。在这个过程中，我经历了无数次的挫折和失败，但也学到了许多原理并积累了宝贵的开发经验。

毕业设计研究期间，我提升了自己动手实践的能力，这让我深切体会到在创造过程中不断探索的困难和成功时的喜悦。在此，我要向那些帮助过我的老师和同学们表示由衷的感激！