Computer Science and Application 计算机科学与应用, 2026, 16(5), 49-57
Published Online May 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.165163

Hans汉斯

基于TabTransformer的网络入侵检测系统研究与实现

易皓天，楼其俊，尹铭宇，林濠浚

宁波工程学院网络空间安全学院，浙江 宁波

收稿日期：2026年4月6日；录用日期：2026年5月8日；发布日期：2026年5月18日

摘　要

随着网络攻击手段日益复杂多样，传统入侵检测方法在复杂流量环境下面临性能瓶颈。针对网络流量数据中高维特征及复杂特征交互问题，文章设计并实现了一种基于TabTransformer的端到端网络入侵检测系统，通过引入特征嵌入和自注意力机制，捕获网络流量数据中复杂的非线性关系。基于CIC-IDS2017和UNSW-NB15公开数据集的对比实验表明，该系统在准确率、F1-Score、PR-AUC等指标上均优于CNN、RNN、LSTM等典型深度学习模型，在两个数据集的F1-Score均达到0.98以上，可为Transformer在入侵检测中的应用提供了一定参考。

关键词

网络安全，攻击检测，流量分析，网络入侵检测，TabTransformer

Research and Implementation of a Network Intrusion Detection System Based on TabTransformer

Haotian Yi, Qijun Lou, Mingyu Yin, Haojun Lin

School of Cyber Science and Engineering, Ningbo University of Technology, Ningbo Zhejiang

Received: April 6, 2026; accepted: May 8, 2026; published: May 18, 2026

Abstract

As the methods of network attacks become increasingly complex and diverse, traditional intrusion detection methods are limited in performance in complex traffic environments. To address the issues

文章引用: 易皓天, 楼其俊, 尹铭宇, 林濠浚. 基于 TabTransformer 的网络入侵检测系统研究与实现[J]. 计算机科学与应用, 2026, 16(5): 49-57. DOI: 10.12677/csa.2026.165163

of high-dimensional features and complex feature interactions in network traffic data, this paper designs and implements an end-to-end network intrusion detection system based on TabTransformer. By introducing feature embedding and self-attention mechanisms, it captures the complex nonlinear relationships in network traffic data. Comparative experiments based on the public datasets CIC-IDS2017 and UNSW-NB15 show that this system outperforms typical deep learning models such as CNN, RNN, and LSTM in terms of accuracy, F1-Score, PR-AUC, etc. The F1-Score of this system in both datasets reaches above 0.98, providing certain references for the application of the Transformer in intrusion detection.

Keywords

Cyber Security, Attack Detection, Traffic Analysis, Network Intrusion Detection, TabTransformer

1. 引言

随着网络安全事件的复杂程度与影响范围持续加剧，入侵检测已成为现代网络防御体系中不可或缺的核心环节。传统的网络入侵检测系统如 Snort、Suricata 等主要依赖基于规则的匹配方法，在面对复杂攻击时检测能力受限[1] [2]。随着机器学习与深度学习的发展，随机森林、SVM、CNN、RNN、LSTM 等方法被广泛用于入侵检测并提升了性能[3]-[6]，但在建模高维流量特征间复杂交互关系方面仍存在不足。Transformer 模型凭借以自注意力机制为主的神经网络架构，在复杂模式建模上表现突出[7] [8]。而 TabTransformer 作为面向表格数据的 Transformer 变体，能够通过特征嵌入和自注意力机制，对类别特征与数值特征间的交互关系进行建模[9]，高度契合入侵检测任务中网络流量的特征形态。

基于此，本文设计并实现了一种基于 TabTransformer 的端到端网络入侵检测系统，并引入了 Focal Loss 损失函数缓解入侵检测中常见的类别不平衡问题，增强对少数攻击类的检测能力[10]。在 UNSW-NB15 [11]和 CIC-IDS2017 [12]两大公开数据集上的实验结果显示，该方法在 Acc、F1-Score 及 PR-AUC 等指标上均优于 CNN、RNN、LSTM 等基线模型。研究表明，TabTransformer 在复杂流量场景下具有良好的有效性与应用潜力。

2. 相关研究

随着网络流量的快速增长和网络攻击手段的持续演化，网络入侵检测已成为网络安全防御体系的研究重点[13]。目前，国内外已经在关键基础设施保护、云原生环境监测、加密流量分析、工业控制系统防护及内部威胁检测等应用领域开展网络入侵检测技术的研究工作[14]。现有方法主要分为基于特征的检测和基于异常的检测两类。基于特征的检测技术如 Snort 和 Suricata 等经典入侵检测系统，主要通过签名库和规则库匹配流量行为并识别攻击[1]。此类方法检测速度较快，但其依赖人工长期频繁维护，实际应用成本较高[15]。基于异常的检测技术通过机器学习或统计方法对网络流量的威胁性进行区分，如基于支持向量机(SVM)的异常检测模型，具备一定未知攻击发现能力，但现有模型漏报与误报率仍较高，检测精度有待提升[16]。

近年来，研究者已将 CNN、RNN 及 LSTM 等多种深度学习模型应用于网络入侵检测任务，并在不同场景中展现出各自优势。CNN 擅长局部特征提取，适合处理数据报文头部特征或固定长度的流量序列，

具有提取效率高、并行计算能力强的特点，但其对流量数据的时序依赖关系和受时间影响较大的长序列流量的分析效果较差[17]。RNN 可建模连续数据包之间的上下文关系，改善了 CNN 对时序信息利用不足的问题，但其在训练过程中易产生梯度消失或梯度爆炸问题，影响长序列网络流量中长期依赖的学习[18]。LSTM 通过门控机制提升了流量数据长时依赖的学习能力，通常比 RNN 在长序列任务上表现更好，但其计算开销较大、训练耗时较长，且对表格化流量统计特征的复杂交互关系建模能力有限[19] [20]。因此，传统模型在复杂结构化流量场景下仍存在提升空间。

Transformer 模型最初用于自然语言处理，其自注意力机制能够建模长距离依赖关系[7]。在此基础上，TabTransformer 将 Transformer 的自注意力机制应用于结构化数据建模，通过对类别特征进行嵌入并在特征空间执行注意力计算，实现对高阶特征交互的有效学习[9]。该方法可更好地融合类别特征与数值特征，弥补传统模型在结构化数据深层交互建模上的不足。在网络流量入侵检测任务中，流量数据的不同特征之间往往存在复杂的关联关系。因而，TabTransformer 能够更充分地提升模型对异常行为模式的建模能力，提升检测性能。基于这一优势，本文将其作为系统的核心检测模型。

3. 系统设计与实现

3.1. 系统总体架构

为了实现从原始网络流量到入侵检测结果的端到端处理，本文设计并实现了一种基于 TabTransformer 的网络入侵检测系统。在当前研究背景下，多数入侵检测模型在依赖结构化表格数据为主的网络流量数据集进行训练，因此这些模型在实际应用的过程中缺乏与真实网络流量间有效的结构化转换流程。针对这一应用障碍，系统设计了标准化特征转换与流式处理流程，从而使 TabTransformer 能够应用于真实流量环境下的网络入侵检测任务中(见图 1)。

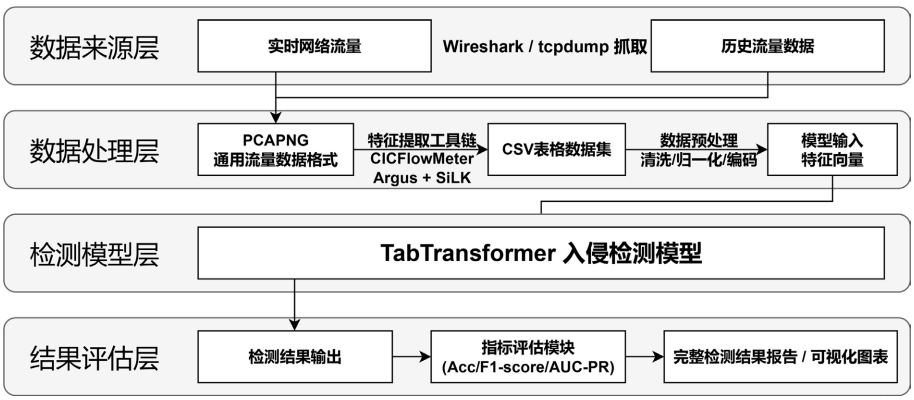

Figure 1. Layered architecture of the TabTransformer-based network intrusion detection system
图 1. 基于 TabTransformer 的网络入侵检测系统分层架构图

3.2. 流量采集与数据预处理

流量采集与预处理是整个检测系统的基础模块，其主要任务是将非结构化的原始报文转换为可被模型用于训练和评估的结构化特征。系统通过 Wireshark、tcpdump 监听网络接口并采集实时流量，实现对实时流量的捕获，并统一存储为 PCAPNG 经典流量报文格式，并引入 Python 第三方库 Scapy 进行数据包的解析，实现对网络层与传输层关键字段的提取，为后续的特征构建提供细粒度的数据支持。

在特征工程阶段，系统集成了 CICFlowMeter、Argus 以及 SiLK 等开源工具链。这些工具能够提取包括数据包长度分布、流持续时间、双向时间间隔以及基于包大小分布的吞吐量等特征。提取后的数据经

过特征映射与对齐后调整为固定维度特征向量，对数值型特征采用 Min-Max 技术归一化至[0, 1]区间。同时通过移除零方差特征以降低计算冗余，并对无穷大值(±inf)及缺失值执行中位数或众数填充，以确保后续模型推理的输入完整性与分布稳定性，从而提升模型收敛速度和检测精度。

3.3. TabTransformer 检测模型设计与实现

检测模型层是本系统的核心计算模块，负责从高维流量特征中识别恶意行为攻击模式。本文采用 TabTransformer 模型，在特征维度上引入自注意力机制以学习特征之间的复杂交互关系(见图 2)。

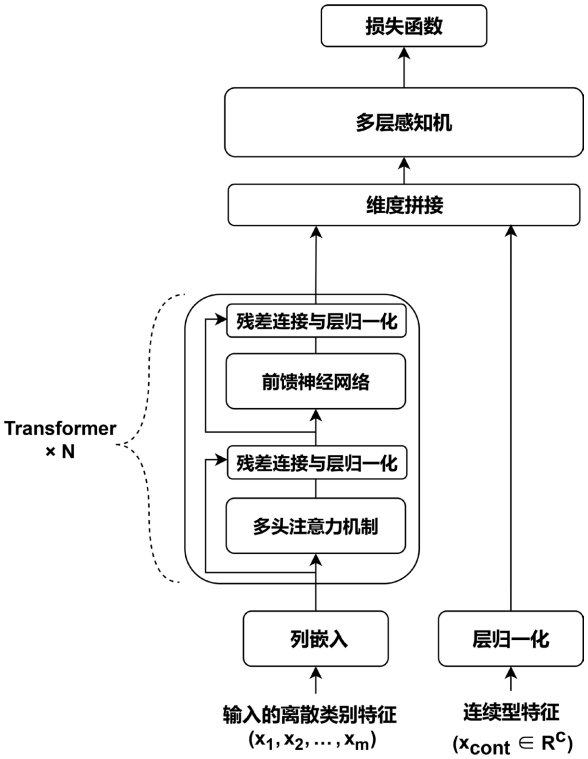

Figure 2. Basic structure diagram of TabTransformer model
图 2. TabTransformer 模型基本结构图

系统的模型实现主要由以下三部分构成：

在特征嵌入与预处理层中，系统对离散类别特征通过列嵌入将其映射为低维稠密向量；对连续型特征则通过层归一化完成维度对齐与预处理。

在 Transformer 编码器层中，系统在获得类别特征的嵌入向量后，模型会将它们视为一个特征序列，并输入到由 N 层堆叠的 Transformer 编码器中。编码器中的多头注意力机制会在所有特征向量之间两两计算注意力权重，从而捕捉流量特征之间的全局交互关系。编码器内部通过残差连接与层归一化稳定训练，并由前馈神经网络完成非线性变换。

在特征聚合与分类输出层中，系统将 Transformer 编码器输出的特征序列与预处理后的连续型特征进行维度拼接，并将拼接后的特征输入多层感知机，最后通过损失函数完成分类。

这种设计使得 TabTransformer 在诸如网络入侵检测等任务上具有天然的适配性。TabTransformer 通过其独特的特征处理方式，针对众多特征字段构成的网络流量的表格型数据，能够无损地将这些信息编码并深度融合，精准地捕获恶意流量中隐藏的复杂特征交互模式，从而构建出高性能的入侵检测模型。

针对网络流量数据普遍存在的类别不平衡问题，本文采用了 Focal Loss [10]作为损失函数，其核心思想是将注意力集中在难分类的稀有攻击样本上，从而缓解类别不平衡带来的性能下降问题：

$$\mathrm{FL}\left(p_t\right)=-\alpha_t\left(1-p_t\right)^{\gamma}\log\left(p_t\right) \tag{1}$$

其中，p_t 是模型对正确类别的预测概率，α_t 是类别权重参数，用于平衡正负样本的重要性，γ 是聚焦参数，用于控制难易样本的权重衰减速率。

3.4. 指标评估与可视化分析

结果评估模块位于系统处理流程的最终阶段，其主要功能是将模型预测值转化为安全分析依据。模块基于混淆矩阵统计，通过对真正例、假正例、真反例及假反例的统计，确立了以准确率(Accuracy)、F1-Score 与 PR-AUC (精确率–召回率曲线下面积)等指标为核心的评价准则。

4. 实验设计与结果分析

4.1. 实验数据与实验设置

为验证所构建入侵检测系统的性能，本文在两个公开数据集 UNSW-NB15 [11]和 CIC-IDS2017 [12]上开展实验评估。上述数据集广泛应用于网络入侵检测研究，能够较为全面地反映多类型攻击场景下的检测能力。UNSW-NB15 数据集采用其 NetFlow 转换版本 NF-UNSW-NB15-v3 [21]，该版本包含约 236 万个样本，每个样本由 53 维特征组成，涵盖了 9 种攻击类型。CIC-IDS2017 数据集包含约 252 万个样本，特征维度为 52 维，涵盖了 6 种攻击类型，是目前网络流量分析研究领域应用最广泛、最能体现系统有效性和泛化能力的基准数据集之一。

为保证数据质量并适配 TabTransformer 模型的输入要求，本文对两个模型训练数据集进行了统一的预处理：首先进行缺失值处理，删除包含空值的样本；其次进行特征筛选，移除冗余特征及方差接近于零的常值特征；接着对数值型特征进行 Min-Max 归一化至[0, 1]区间，将 2 个类别型特征采用标签编码(Label Encoding)将其转换为整数形式，并与 52 维数值特征拼接，总共为 54 维以供后续嵌入层使用。

在模型配置方面，实验环境基于 Python 和 PyTorch 框架实现，实验数据集按照 90%训练集，5%验证集，5%测试集的比例进行划分，TabTransformer 采用 8 层 Transformer 编码器结构，每层包含 16 个注意力头，嵌入维度设置为 128，前馈网络维度为 512。模型训练采用 AdamW 优化器，初始学习率设置为 5e−5，采用余弦退火学习率调度策略。CNN、RNN 和 LSTM 三类基线模型分别采用 3 层结构网络嵌套，并对流量数据集做适配，CNN 将输入重构为单通道一维序列，RNN 与 LSTM 均先通过 Linear (F, 256)将输入投影到 256 维隐藏空间。训练过程中综合监控验证集上的 Focal Loss 和 Accuracy，当两者结合分数最优时保存模型权重作为最终模型。

4.2. 评估指标

4.2.1. F1-Score

针对网络流量数据中严重的类别不平衡问题，单纯依靠准确率(Accuracy)难以全面反映模型对少数类攻击样本的检测能力。因此，本文引入 F1-Score 作为核心评价指标，其公式如下：

$$\mathrm{F1}=2\cdot\frac{\mathrm{Precision}\cdot\mathrm{Recall}}{\mathrm{Precision}+\mathrm{Recall}} \tag{2}$$

其中，Precision (精确率)表示预测为攻击样本中实际为攻击的比例，Recall (召回率)表示实际攻击样本中被正确识别的比例。F1-Score 通过对精确率与召回率进行调和平均，在兼顾误报率与漏报率的同时，能

够有效衡量模型在不平衡数据场景下的整体检测性能。

4.2.2. PR-AUC (AP)

为进一步评估模型在不同分类阈值下的性能表现，本文引入精确率–召回率曲线下面积(PR-AUC)作为辅助评价指标。PR 曲线以召回率为横轴、精确率为纵轴，通过对不同阈值下的预测结果进行统计绘制得到，其面积可表示为：

$$\mathrm{PR}-\mathrm{AUC}=\int_0^1 \mathrm{Precision}\left(\mathrm{Recall}\right)d\left(\mathrm{Recall}\right)\approx\sum_{i=1}^{n}\mathrm{Precision}_i\cdot\Delta\mathrm{Recall}_i \tag{3}$$

PR-AUC 能够反映模型在不同召回水平下的精确率变化情况，特别适用于类别分布不均衡的任务场景。相比于准确率等整体指标，PR-AUC 更加关注少数类(攻击流量)的识别能力，因此能够更客观地评估入侵检测系统对异常流量的检测性能。

4.3. 训练结果

为验证所提出系统的有效性，本文在 UNSW-NB15 和 CIC-IDS2017 两个公开数据集上进行了实验，并将 TabTransformer 架构与 CNN、RNN 及 LSTM 等典型深度学习方法进行了对比。所有实验均在同一软硬件环境下进行，并采用一致的数据预处理流程与训练参数配置，以保证实验结果的公平性。

最终，采用 Accuracy、F1-Score 和 PR-AUC 对训练结果进行评估，对各模型在两个数据集上的性能进行对比分析，实验结果如表 1~3 所示。

Table 1. Mean Acc values of detection model
表 1. 检测模型的 Acc 均值

模型\数据集	NF-UNSW-NB15	CIC-IDS2017
CNN	0.964	0.9383
RNN	0.9424	0.963
LSTM	0.936	0.9762
TabTransformer	**0.9852**	**0.9848**

Table 2. Mean F1-Score values of detection model
表 2. 检测模型的 F1-Score 均值

模型\数据集	NF-UNSW-NB15	CIC-IDS2017
CNN	0.9604	0.9042
RNN	0.9401	0.953
LSTM	0.9441	0.97
TabTransformer	**0.9838**	**0.9808**

Table 3. Mean PR-AUC values of detection model
表 3. 检测模型的 PR-AUC 均值

模型\数据集	NF-UNSW-NB15	CIC-IDS2017
CNN	0.9668	0.9894
RNN	0.9127	0.9957
LSTM	0.955	0.9962
TabTransformer	**0.9901**	**0.9976**

为进一步分析模型对不同攻击类型的检测能力，本文对比了各模型在 CIC-IDS2017 数据集中六种攻击类型上的 F1-Score 值(见表 4)。

Table 4. The F1-Scores of each model on different attack types in CIC-IDS2017
表 4. 各模型在 CIC-IDS2017 不同攻击类型上的 F1-Score

攻击类型\模型	CNN	RNN	LSTM	**TabTransformer**
DDoS	0.8212	0.9362	0.9792	**0.9974**
Port Scanning	0.8012	0.8493	0.8349	**0.8536**
Brute Force	0.3038	0.8507	0.9339	**0.954**
DoS	0.762	0.8583	0.9339	**0.9731**
Web Attack	0.2173	0.2953	0.2997	**0.3953**
Bots	0.2077	0.4811	0.4	**0.4299**

4.4. 实验结果分析

从表 1~3 的实验结果可以看出，本文所构建的基于 TabTransformer 的入侵检测系统在两个数据集上均取得了优于对比模型的性能。在 NF-UNSW-NB15 数据集上，TabTransformer 的 F1-Score 达到 0.9838，相较于表现最优的对比模型(LSTM)提升约 3.9%；在 CIC-IDS2017 数据集上，其 F1-Score 达到 0.9808，相较于 LSTM 提升约 1.1%。在 PR-AUC 指标上，TabTransformer 分别达到 0.9901 和 0.9976，整体优于 CNN、RNN 及 LSTM 模型，表明其在不平衡数据场景下对少数类攻击具有更稳定的识别能力。

上述性能提升一方面得益于 TabTransformer 对表格数据特征间复杂交互关系的建模能力。相比于 CNN 主要关注局部特征模式，或 LSTM 侧重时间序列依赖关系，TabTransformer 通过自注意力机制能够在全局范围内动态建模不同特征之间的关联性，从而更有效地捕捉网络攻击行为中的组合特征模式。另一方面，Focal Loss 的引入在一定程度上缓解了类别不平衡问题，使模型在训练过程中更加关注难分类样本，从而提升了整体检测性能。

从表 4 中不同攻击类型的检测结果可以进一步观察到，TabTransformer 在 DDoS、DoS 及 Brute Force 等典型攻击类型上表现出较高的检测精度，F1-Score 均超过 0.95。然而，对于 Web Attack 和 Bots 等攻击类型，各模型整体表现均相对较低，其中 TabTransformer 虽优于其他模型，但 F1-Score 仍不足 0.5。这一现象表明，此类攻击在特征空间中与正常流量具有较高相似性，导致模型难以有效区分。此外，这也反映出当前基于流量统计特征的方法在处理隐蔽攻击行为时仍存在一定局限性。

综上所述，TabTransformer 在网络流量入侵检测任务中表现出较强的性能优势，尤其在复杂特征关系建模及不平衡数据处理方面具有明显优势。但在部分隐蔽攻击类型上的检测能力仍有待进一步提升，这为后续研究提供了改进方向。

4.5. 模型可解释性分析

为进一步提高模型决策过程的可解释性，本文基于 CIC-IDS2017 测试集对 TabTransformer 模型进行了特征重要性分析。具体而言，采用特征置乱(Permutation Importance)方法，逐一随机打乱各数值特征的取值，并以模型宏平均 F1 值的下降幅度衡量对应特征对分类结果的贡献程度。在此基础上，统计并绘制 Top-10 数值特征重要性结果(见图 3)。

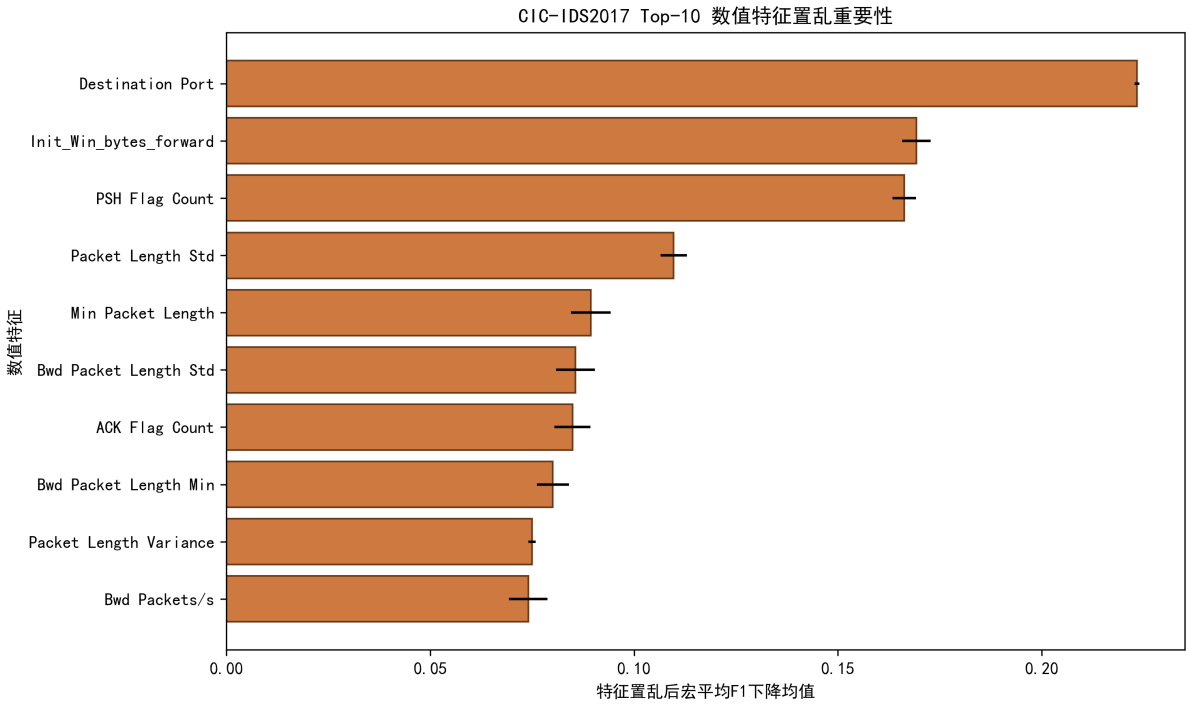

Figure 3. Top-10 importance of numerical feature characteristics
图 3. Top-10 数值特征重要性

从图 3 可以看出，Destination Port、Init_Win_bytes_forward、PSH Flag Count 等特征的重要性较高，在被打乱后均会引起模型宏平均 F1 值的明显下降，部分特征对应的性能降幅超过 15%。这表明 TabTransformer 并非依赖随机噪声进行分类，而是学习到了具有较强判别能力的流量统计特征。进一步说明，模型在攻击识别过程中能够自主倾向性地有效利用端口信息、窗口字节特征及报文标志位等关键属性，从而为其检测结果提供一定的可解释性支持。

5. 结语

本文围绕网络流量入侵检测任务，设计并实现了一种基于 TabTransformer 的网络入侵检测系统，该系统将 Transformer 的自注意力机制引入表格型流量数据建模过程中，通过对特征间复杂交互关系的建模，提高了对异常流量的识别能力。实验结果表明，系统所集成的 TabTransformer 模型在多个数据集上均取得了较好的检测性能，在多类攻击识别任务中表现出良好的准确性与稳定性。

尽管取得了一定效果，本文方法仍存在一定局限性。例如，在 Web 攻击与机器人攻击等行为特征较为隐蔽的场景下，模型检测性能仍有提升空间。这主要是由于此类攻击与正常流量在特征空间中存在较高相似性，增加了模型判别难度。未来可从特征增强、模型结构优化以及引入时序信息等方面进一步提升检测能力。

综上所述，本文对 TabTransformer 在网络流量入侵检测中的应用进行了探索，并构建了完整的检测系统，为基于 Transformer 的入侵检测系统设计提供了一定参考。后续工作可进一步结合实际网络环境，开展实时检测与系统优化研究，以提升系统的实用性与推广价值。

基金项目

国家级大学生创新创业训练项目(202511058021)。

参考文献

[1] Qutqut, M.H., Ahmed, A., Taqi, M.K., Abimanyu, J., Ajes, E.T. and Alhaj, F. (2026) A Comparative Evaluation of Snort and Suricata for Detecting Data Exfiltration Tunnels in Cloud Environments. *Journal of Cybersecurity and Privacy*, **6**, Article 17. https://doi.org/10.3390/jcp6010017

[2] Hozouri, A., Mirzaei, A. and Effatparvar, M. (2025) A Comprehensive Survey on Intrusion Detection Systems with Advances in Machine Learning, Deep Learning and Emerging Cybersecurity Challenges. *Discover Artificial Intelligence*, **5**, Article No. 314. https://doi.org/10.1007/s44163-025-00578-1

[3] 张洁, 张永. 一种基于核心向量机的分层入侵检测模型[J]. 计算机应用与软件, 2024, 41(7): 296-301, 314.

[4] 王雪妍, 温蜜, 李晋国, 等. 一种卷积神经网络结合特征融合的网络入侵检测方法[J]. 计算机应用与软件, 2024, 41(8): 359-366.

[5] 黄亮, 陶达, 王秀木, 等. 基于改进 LSTM 的网络入侵检测方法[J]. 计算机测量与控制, 2025, 33(2): 63-70.

[6] Dash, N., Chakravarty, S., Rath, A.K., Giri, N.C., AboRas, K.M. and Gowtham, N. (2025) An Optimized LSTM-Based Deep Learning Model for Anomaly Network Intrusion Detection. *Scientific Reports*, **15**, Article No. 1554. https://doi.org/10.1038/s41598-025-85248-z

[7] Vaswani, A., Shazeer, N., Parmar, N., *et al*. (2017) Attention Is All You Need. arXiv: 1706.03762.

[8] Neto, E.C.P., Iqbal, S., Buffett, S., Sultana, M. and Taylor, A. (2025) Deep Learning for Intrusion Detection in Emerging Technologies: A Comprehensive Survey and New Perspectives. *Artificial Intelligence Review*, **58**, Article No. 340. https://doi.org/10.1007/s10462-025-11346-z

[9] Huang, X., Khetan, A., Cvitkovic, M., *et al*. (2020) TabTransformer: Tabular Data Modeling Using Contextual Embeddings. arXiv: 2012.06678.

[10] Lin, T., Goyal, P., Girshick, R., He, K. and Dollar, P. (2017) Focal Loss for Dense Object Detection. 2017 *IEEE International Conference on Computer Vision* (*ICCV*), Venice, 22-29 October 2017, 2999-3007. https://doi.org/10.1109/iccv.2017.324

[11] Moustafa, N. and Slay, J. (2015) UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). 2015 *Military Communications and Information Systems Conference* (*MilCIS*), Canberra, 10-12 November 2015, 1-6. https://doi.org/10.1109/milcis.2015.7348942

[12] Sharafaldin, I., Habibi Lashkari, A. and Ghorbani, A.A. (2018) Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the* 4*th International Conference on Information Systems Security and Privacy*, Funchal, Madeira, 22-24 January 2018, 108-116. https://doi.org/10.5220/0006639801080116

[13] Akuthota, U.C. and Bhargava, L. (2025) The Role of Machine and Deep Learning in Modern Intrusion Detection Systems: A Comprehensive Review. *Computers and Electrical Engineering*, **124**, Article ID: 110318. https://doi.org/10.1016/j.compeleceng.2025.110318

[14] 蹇诗婕, 卢志刚, 杜丹, 等. 网络入侵检测技术综述[J]. 信息安全学报, 2020, 5(4): 96-122.

[15] Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R. and Madinabeitia, G. (2022) On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. *Applied Sciences*, **12**, Article 852. https://doi.org/10.3390/app12020852

[16] Kumar, L.K.S., Nethi, S.R., Uyyala, R., Vurubindi, P., Narahari, S.C., Das, A.K., *et al*. (2026) Anomaly-Based Intrusion Detection on Benchmark Datasets for Network Security: A Comprehensive Evaluation. *Scientific Reports*, **16**, Article No. 8507. https://doi.org/10.1038/s41598-026-38317-w

[17] Ali, M.L., Thakur, K., Schmeelk, S., Debello, J. and Dragos, D. (2025) Deep Learning Vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study. *Applied Sciences*, **15**, Article 1903. https://doi.org/10.3390/app15041903

[18] Zhang, Y., Muniyandi, R.C. and Qamar, F. (2025) A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance. *Applied Sciences*, **15**, Article 1552. https://doi.org/10.3390/app15031552

[19] 张昊, 张小雨, 张振友, 等. 基于深度学习的入侵检测模型综述[J]. 计算机工程与应用, 2022, 58(6): 17-28.

[20] Borisov, V., Leemann, T., Seßler, K., Haug, J., Pawelczyk, M. and Kasneci, G. (2024) Deep Neural Networks and Tabular Data: A Survey. *IEEE Transactions on Neural Networks and Learning Systems*, **35**, 7499-7519. https://doi.org/10.1109/tnnls.2022.3229161

[21] Luay, M., Layeghy, S., Hosseininoorbin, S., *et al*. (2025) Temporal Analysis of NetFlow Datasets for Network Intrusion Detection Systems. arXiv: 2503.04404.