基于深度学习的电商恶意攻击行为识别与防御系统设计

王辰
天津大学（仁爱学院），邮政储蓄银行信用卡中心(智慧营销项目)，北京国信创新科技股份有限公司(项目部)
DOI:10.12238/acair.v3i3.15595

[摘　要] 近年来,随着网络的广泛运用,电子商务已经成为主流的商业贸易方式。与此同时,电商企业的网络安全隐患也日益严峻,各种网络攻击事件层出不穷。深度学习技术因其强大的特征学习与泛化能力,为构建高效的攻击识别与防御系统提供了全新路径。本文围绕电商平台的核心安全需求,基于用户行为数据建模与攻击类型特征分析,设计了一套融合CNN、LSTM与注意力机制的多维深度识别模型,并结合策略响应引擎实现了具备实时性与可扩展性的自动化防御系统。实证应用表明,该方案在识别精度、误报控制与系统适配性方面具有良好的工程效果与推广价值。
[关键词] 电商安全；深度学习；恶意行为识别；自动化防御；行为建模
中图分类号：B848.5　**文献标识码：**A

Design of E-commerce Malicious Attack Behavior Identification and Defense System Based on Deep Learning

Chen Wang
Tianjin University (Ren'ai College), Postal Savings Bank Credit Card Center (Smart Marketing Project), Beijing Guoxin Innovation Technology Co., Ltd. (Project Department)

[Abstract] In recent years, with the widespread use of the Internet, e-commerce has become the mainstream mode of commercial trade. At the same time, the network security risks of e-commerce companies are becoming increasingly serious, and various cyber attack incidents are emerging one after another. Deep learning technology provides a new path for building efficient attack identification and defense systems due to its powerful feature learning and generalization capabilities. Focusing on the core security requirements of e-commerce platforms, this paper designs a multi-dimensional deep recognition model integrating CNN, LSTM and attention mechanism based on user behavior data modeling and attack type feature analysis, and combines the policy response engine to realize an automated defense system with real-time and scalability. The empirical application shows that the scheme has good engineering effect and promotion value in terms of recognition accuracy, false alarm control and system adaptability.
[Key words] e-commerce security; deep learning; identification of malicious behavior; automated defense; Behavioral modeling

引言

电商平台在数字经济中扮演着关键角色,但伴随业务规模扩大和用户活跃度提高,各类网络攻击行为也呈现出快速蔓延的趋势。攻击者通过模拟正常用户操作,伪装行为特征,规避传统安全策略,使得电商系统面临用户数据泄露、交易信用破坏和平台资源滥用等严重风险。以往依赖人工规则、黑名单过滤或简单阈值判断的方式,已难以应对当前攻击技术的智能化与动态化发展。如何在保障平台性能与用户体验的前提下,实现高效、精准、可持续的攻击识别与防御,成为当前网络安全技术面临的重要课题。

1 电商平台常见恶意攻击行为分析

在电商系统高度依赖用户行为与数据交互的背景下,平台安全正面临日益复杂的挑战。各类恶意攻击行为不断演化,从最初的简单脚本操作发展为具备高度伪装性与智能策略的复合式攻击,对交易环境的公正性、用户信息的隐私性以及平台资源的可用性构成严重威胁。虚假交易通过模拟正常购买流程制造虚假销量与评价,破坏平台信用体系;自动化爬虫借助高频访问机制窃取敏感信息,扰乱正常业务流量；DDoS借助客户/服务器(C/S)技术将处于不同位置的多个攻击者联合起来同时向一个或多个目标发动攻击,通过分析目标集群的漏洞,进入后门控制

主机,进行集中管理,采用不同的攻击方式手段向目标主机发起攻击[1]。而账户盗用攻击往往借助撞库、钓鱼等手段非法获取用户身份,进而实施高风险操作。

2 电商恶意行为识别中的深度学习关键技术

在电商安全体系中,深度学习技术以其强大的特征建模与非线性表达能力,逐渐成为识别复杂恶意行为的重要工具。针对电商场景中多样化的攻击模式,模型选择需依据行为特征、数据结构与攻击类型进行精确适配。卷积神经网络(CNN)适用于处理用户点击路径或跳转行为的空间模式识别,循环神经网络(RNN/LSTM)则在捕捉用户操作的时序规律方面表现出色,能够挖掘慢速爬虫、分时刷单等策略性攻击中的行为演变特征。图神经网络(GNN)通过构建用户、设备与资源节点之间的图结构,有效识别跨账号、跨终端的协同攻击;而Transformer结构则借助全局自注意力机制提升对长序列、多维交互行为的解析能力,适用于多类行为重叠场景下的关键节点提取[2]。为实现深度模型的有效训练,数据建模与预处理策略至关重要。平台通过日志系统采集包括用户请求、设备指纹、行为时间等在内的高频行为数据,并基于滑动窗口构建行为序列,提取访问频率、跳转路径、停留时长等统计特征,同时对离散字段进行嵌入编码处理。

3 基于深度学习的恶意攻击识别模型设计

3.1模型结构设计

识别模型采用多通道输入结构,融合用户行为序列、设备信息与操作环境特征。底层通过LSTM捕捉行为时序关系,嵌入层处理离散属性如IP段、设备类型并统一归一化。为识别协同攻击行为,构建用户－资源－设备图谱,输入图神经网络提取节点间的结构依赖。中层引入注意力机制,对操作序列中关键行为赋予更高权重,提升对潜在攻击意图的关注。融合层拼接多源特征,接入全连接网络输出多类攻击识别结果。模型支持TensorRT轻量化部署,兼容高并发实时检测需求,适用于平台在真实场景中的快速响应与精准拦截。

3.2训练策略与评估体系

在模型训练过程中,合理的策略设定与评估机制是确保识别系统性能稳定与泛化能力强的关键环节。训练目标采用带权重的多分类交叉熵损失函数,对类别不均衡问题进行有效抑制[3]。设定类别总数为C,第i类的样本权重为w_i,样本标签为y_i,预测概率为pi,则损失函数表达式为:

$$L=-\sum_{i=1}^{C} w_i \cdot y_i \cdot \log(p_i) \tag{1}$$

其中,w_i根据样本频率设置为:$w_i=\frac{1}{\log(1+n_i)}$,$n_i$为第i类样本数量,以抑制主类对损失主导的倾向。数据划分采用8:1:1的训练、验证、测试比例,确保分布均衡,且每轮训练采用随机采样,打乱行为序列顺序以提升模型鲁棒性。

为加快收敛速度与优化性能,训练中引入学习率预热与余弦退火机制。预热阶段线性增长学习率至设定值ηmax,后续训练轮次中按照如下公式逐步衰减:

$$\eta_t=\eta_{\min}+\frac{1}{2}(\eta_{\max}-\eta_{\min})\left(1+\cos(\frac{t}{T}\pi)\right) \tag{2}$$

其中,η_t为第t轮学习率,T为总训练轮数,保证初期充分探索、后期稳定收敛。训练过程使用Adam优化器,批次大小设置为64,最大迭代轮数为120轮,每轮后进行验证集评估,并记录F1分数与AUC变化。

模型评估体系采用多维指标联合判定:准确率(Accuracy)、召回率(Recall)、精确率(Precision)、F1值与AUC。其中,F1值作为主要参考指标,用以衡量在少数类识别场景中的平衡性,其计算公式为:

$$F1=2\cdot\frac{\mathrm{Pr}ecision\cdot\mathrm{Re}call}{\mathrm{Pr}ecision+\mathrm{Re}call} \tag{3}$$

训练日志记录每轮损失变化与指标表现,并结合混淆矩阵对具体类别的识别偏误进行定位。最终,选取在验证集上F1值与AUC综合最优的模型参数用于部署,确保系统在实际运行中具备稳定的识别性能与误报控制能力。

3.3多类攻击联合识别机制

面对电商平台中多样化的攻击类型,模型需要具备同时识别多类攻击的能力,并能够处理不同攻击之间的模糊边界与行为重叠问题。为此,识别系统引入多任务学习机制,将多类攻击识别转化为联合分类问题与风险评分问题的融合建模。在模型结构中,通过共享底层编码器提取统一特征表示,再分别接入多个任务分支,实现并行输出。

分类任务部分采用多标签Sigmoid输出而非Softmax,允许样本同时属于多个攻击类别。例如,若某一行为同时涉及异常登录与爬虫行为,标签为$y=[1,1,0,0]$对应攻击类型分别为登录劫持、爬虫、刷单、DDoS。其多标签二元交叉熵损失函数定义为:

$$L_{multi}=-\sum_{i=1}^{C}\left[y_i\cdot\log(p_i)+(1-y_i)\cdot\log(1-p_i)\right] \tag{4}$$

其中,C为攻击类型数量,y_i为第i类标签,p_i为模型预测概率。该方式支持多重攻击标签共存,适配复杂行为样本。

为辅助分类判断,模型同时引入攻击风险得分预测模块,输出攻击概率值$s\in[0,1]$,用于量化样本整体威胁程度。该得分通过特征向量h与权重向量w点积后接Sigmoid函数计算得出:

$$s=\sigma(w^T h+b) \tag{5}$$

模型推理阶段，将类别预测结果与风险得分联合作为判断依据，当$s>\theta$且存在任一攻击标签概率$p_i>\delta$时，触发响应策略。该机制可以提升模型对攻击边缘行为的敏感性，强化对轻量级、隐蔽型复合攻击的识别能力，保证系统在多样化攻击环境下具备较强的判别鲁棒性与场景适应力。

4 电商恶意攻击防御系统设计与实现

4.1系统总体架构设计

电商恶意攻击防御系统采用分层解耦式架构，围绕“识别+分发+联动响应”的核心流程构建业务闭环。在整体结构中，用户请求统一接入“安全接入网关与请求调度中心”，由“请求类型判断+攻击识别引擎集成模块”进行初步分析与判别。系统通过逻辑分流将静态类请求（如商品展示图、详情页等）直接引导至“CDN缓存系统+静态内容渲染服务”，实现免识别通道，有效减轻识别压力。

针对动态类请求，系统将其引入“动态请求行为判别与识别模型入口”，调用深度学习模型对访问序列、行为特征进行向量建模与攻击类型分类[4]。如图1所示，系统从请求接入、识别建模到策略联动响应，形成完整的攻击识别与防御闭环。

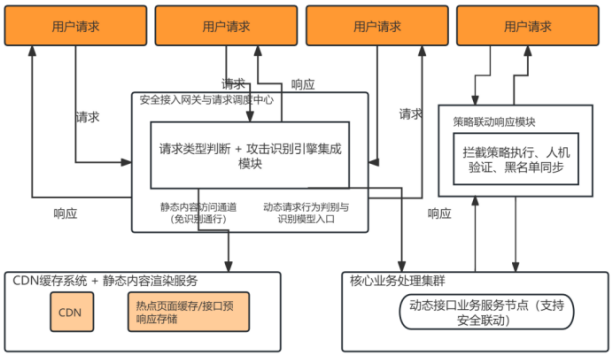

图1 电商平台恶意攻击防御系统总体架构图

4.2自动化响应机制与防御策略

在完成攻击行为识别后，防御系统必须迅速做出决策并精准执行响应，以实现实战意义上的闭环控制。为此，平台在识别模块输出结果的基础上，构建自动化联动策略体系，聚焦请求拦截、人机识别、流量控制三个维度展开防御操作。系统通过统一的策略执行引擎对识别结果进行分级处理：高风险请求（如命中攻击特征行为图谱）立即进入黑名单队列，触发拦截策略并阻断后续通信链路；中风险请求则自动接入人机验证流程，结合验证码滑动行为、鼠标轨迹分析等机制判断用户行为真实性；低风险请求则动态调整访问频率，通过限速控制平稳接入业务处理节点。该响应策略由“策略联动响应模块”集中调度，与攻击识别结果实现API层级的紧耦合，通过实时策略推送接口将响应规则动态下发至前端接入层与业务后端，保障执行效率与控制粒度。系统预置多套防御模板，支持按攻击类型进行策略定制，如对典型刷单行为启用交易冻结与行为隔离，对DDoS流量采用自动限流+CDN缓存扩散处理策略。

4.3系统部署方案与可扩展性考虑

为确保恶意攻击识别与防御系统在电商业务中稳定运行，平台采用分布式部署架构，将识别模型服务、策略响应引擎与业务服务解耦部署至多个独立节点。系统支持容器化运行，基于Docker与Kubernetes进行模块封装与资源调度，使识别引擎可按需水平扩展，适配促销高峰期的大流量访问场景。模型推理服务通过TensorRT加速部署，嵌入Nginx网关层异步调用，避免对主业务请求路径造成阻塞，保障系统实时性[5]。识别模块与业务系统间通过RESTful API进行数据交互，策略响应结果通过统一网关推送至前端组件与后端服务模块，形成响应闭环。各模块均支持灰度发布与热更新，保障系统在模型迭代与策略调整过程中的业务连续性与风险可控性。对于大规模部署场景，系统提供统一配置管理中心与日志审计模块，实现多节点一致性维护与攻击行为可追溯。

5 结语

本研究面向电商平台面临的多样化、智能化攻击威胁，系统构建了一套基于深度学习的识别与防御体系，从模型结构设计到系统部署联动，均围绕“精准识别、快速响应、灵活扩展”展开技术路径。通过引入时序建模、图结构分析与注意力机制，提升了对复杂行为模式的捕捉能力；结合自动化策略执行与模块化部署，保障了系统在高并发场景下的实用性与可维护性。整体方案不仅实现了恶意攻击的识别分类与响应控制闭环，也为构建安全、高韧性的电商业务环境提供了切实可行的工程支撑。

[参考文献]

[1]刘冬晖,谢佳睿.人工智能网络算法在网络信息处理中的应用研究[J].信息记录材料,2025,26(07):91-93.

[2]张宇,郭文忠,林森,等.深度学习与知识推理相结合的研究综述[J].计算机工程与应用,2022,58(01):56-69.

[3]贺育斌.人工智能技术在电商平台风险控制中的应用与实践研究[J].商展经济,2024,(22):67-70.

[4]马鑫,王芳,段刚龙.面向电商内容安全风险管控的协同过滤推荐算法研究[J].情报理论与实践,2022,45(10):176-187.

[5]肖帅帅,蔡晶晶,郭敏,等.系统安全防护中的业务逻辑漏洞检测与防御策略[J].信息网络安全,2021,(S1):239-242.

作者简介：

王辰(1997--),男,汉族,天津人,本科,研究方向：计算机技术。