引用格式:王晨巍,黎歆雨,高大伟,等. 基于 PSO-LightGBM 的网络资产脆弱性评估模型[J]. 信息对抗技术,2023, 2(2):54-65. [WANG Chenwei, LI Xinyu, GAO Dawei, et al. Vulnerability assessment model of network assets based on PSO-LightGBM[J]. Information Countermeasure Technology, 2023, 2(2):54-65. (in Chinese)]

基于 PSO-LightGBM 的网络资产脆弱性评估模型

王晨巍[1],黎歆雨[1],高大伟[2],沈 毅[3*],李 萌[1]

(1. 合肥工业大学计算机与信息学院,安徽合肥 230009;
2. 中央军委审计署,北京 100036; 3. 国防科技大学电子对抗学院,安徽合肥 230037)

摘 要 随着网络空间资产探测技术的不断发展,越来越多的资产脆弱面暴露在公众面前,在一定程度上增加了网络资产的安全风险。对网络资产进行脆弱性评估,可以及时发现脆弱性较强的高危资产,在安全事件未发生时主动对脆弱的网络资产进行保护和修复,从而有效降低网络安全事件发生的概率。现有研究主要集中在网络资产漏洞评估及网络系统脆弱性评估上,对网络资产脆弱性评估方法的研究还比较匮乏。为了更好地保护网络资产安全,提出了一种基于粒子群优化算法-轻型梯度提升机(particle swarm optimization-light gradient boosting machine, PSO-LightGBM)的网络资产脆弱性评估模型。首先,依据行业标准和专家经验,提出针对网络资产脆弱性的评估指标体系,并根据从网络中爬取的网络资产数据,经预处理后构建了具有 12 个属性特征、11 类标签值的网络资产脆弱性评估数据集;其次,将 PSO 算法与 LightGBM 模型相结合,利用机器学习方法实现网络资产脆弱性的自动化评估;最后,通过实验对比了几种机器学习模型在数据集上的表现,结果表明,基于 PSO-LightGBM 的网络资产脆弱性评估模型的评估准确率可以达到 91.24%,充分验证了该模型的有效性。

关键词 网络安全;网络空间资产;脆弱性评估;轻型梯度提升机;粒子群优化算法

中图分类号 TP 393 **文章编号** 2097-163X(2023)02-0054-12

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2023.02.005

Vulnerability assessment model of network assets based on PSO-LightGBM

WANG Chenwei[1], LI Xinyu[1], GAO Dawei[2], SHEN Yi[3*], LI Meng[1]

(1. School of Computer and Information, Hefei University of Technology, Hefei 230009, China;
2. Audit Office of Central Military Commission of People's Republic of China, Beijing 100036, China;
3. College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China)

Abstract With the development of cyberspace assets detection technology, more and more vulnerable assets are exposed to the public, which will increase the security risk of cyber assets to a certain extent. Vulnerability assessment of network assets can help people discover vulnerable and high-risk assets in time, and proactively protect and repair vulnerable network assets when security events do not occur, which can effectively reduce the probability of network security events. The existing researches mainly focus on the vulnerability assessments of the network assets and the network system, but rarely on the vulnerability assessment

收稿日期:2023-01-13 **修回日期**:2023-02-11

通信作者:沈毅,E-mail:shenyi@nudt.edu.cn

基金项目:网络空间安全态势感知与评估安徽省重点实验室开放课题资助项目(CSSAE-2021-009)

methods. In order to better protect the security of network assets, a vulnerability assessment model of network assets based on particle swarm optimization algorithm-light gradient boosting machine (PSO-LightGBM) was proposed. First, according to the industry standards and expert experiences, an evaluation index system for vulnerability of network assets was proposed. On the basis of the network asset data crawled from the network, a network asset vulnerability assessment data set with 12 attribute characteristics and 11 types of label values was constructed after pretreatment. Then, light gradient boosting machine (LightGBM) model was combined with particle swarm optimization (PSO) algorithm to realize automatic vulnerability assessment of network assets by machine learning method. Finally, the effectiveness of the network asset vulnerability assessment model based on PSO-LightGBM was verified by comparing the performance of several machine learning models on the data set. The experimental results show that this model can accurately assess the vulnerability of network assets, with an accuracy of 91.24%.

Keywords　network security; cyberspace assets; vulnerability assessment; light gradient boosting machine (LightGBM); particle swarm optimization (PSO) algorithm

0　引言

当前，大数据、云计算、物联网、人工智能、区块链等新技术不断涌现，人类社会加速进入数字经济时代[1]。然而，信息技术的进步也为网络安全管理带来了更大的压力，频繁发生的网络攻击等安全事件，极大地增加了全球的网络安全风险。网络资产作为网络安全产业的重要一环，已引起了学术界和工业界的广泛关注，目前相关研究主要集中在网络空间资产测绘技术[2-3]方面。由资产测绘而获取的网络资产数据为网络资产安全管理提供了丰富的数据支持，这对掌握网络空间资源状况，保障网络空间安全防御能力起到了重要的支撑作用。网络资产的脆弱性是指网络资产暴露在互联网中的缺陷与不足，且会对网络资产造成直接或者间接的危害。随着对网络空间资产探测的不断深入，网络资产的脆弱性也逐渐暴露在公众面前，若不能得到及时的保护和修复，一旦遭受网络攻击，将造成难以想象的后果和损失。因此，有必要针对网络资产进行脆弱性评估，以及时发现并保护脆弱程度较高的资产，降低脆弱资产被攻击的可能性，从而减少安全事件的发生。

当前，针对网络资产脆弱性评估的相关研究，主要侧重于对漏洞威胁的评估和网络信息系统的脆弱性评估。对漏洞评估的研究，最具有代表性的是通用漏洞评分系统[4](common vulnerability scoring system，CVSS)，该系统依据专家经验对某一漏洞的严重性从 3 个层次进行评估，并对漏洞自身的严重性进行排序[5]。文献[6]在 CVSS 系统的基础上，融合多个开源的网络安全存储库中的漏洞数据，提出一种基于机器学习的漏洞严重程度评估方法，解决了不同版本 CVSS 评分的兼容性问题。文献[7]进一步考虑了漏洞之间的相关性，并提出了一种定量漏洞评估方法。文献[8]基于动态攻击和防御博弈理论，提出了一种信息网络漏洞威胁评估模型。对于网络系统的脆弱性评估，目前以基于模型的评估为主要趋势。文献[9]以攻击图模型为基础，利用节点的重要性、节点的可达概率以及节点对网络产生的影响作为网络脆弱性的度量指标，建立了网络脆弱性量化计算模型。文献[10]构建了一种通用的网络攻击树模型，通过分析各网络节点的脆弱性，进行网络系统风险发生概率的预测与分析。文献[11]提出一种基于模糊 Petri 网的信息系统安全态势评估模型，可实现对系统安全状况的准确分级。但上述研究均缺乏对网络资产属性完整性的关注，网络资产数据具有丰富的属性信息，基于漏洞的评估方法仅注重对漏洞相关信息的分析，忽略了网络资产的其他属性可能暴露出的脆弱性；基于网络脆弱性的评估方法，从网络系统的攻击与防御角度出发，侧重于对网络整体抵御风险能力的评估，缺少对网络中存在的网络资产信息的深入发掘。因此，上述 2 种方法并不

适用于网络资产脆弱性的评估。

为解决网络资产脆弱性评估问题，本文基于行业标准与专家经验，提出针对网络资产的脆弱性评估指标体系，通过爬取的真实网络资产数据，建立网络资产脆弱性评估数据集，并利用轻型梯度提升机（light gradient boosting machine LightGBM）机器学习模型与粒子优化算法（particle swarm optimization，PSO），构建了一种基于粒子群优化算法-轻型梯度提升机（PSO-LightGBM）的网络资产脆弱性评估模型，实现网络资产脆弱性的自动评估。通过优先对具有较高脆弱性的网络资产进行安全维护，减少了安全事件发生的概率。实验验证了本文提出的模型对网络资产脆弱性评估的有效性。

1 基本原理

1.1 LightGBM 算法

梯度提升决策树（gradient boosting decision tree，GBDT）是目前机器学习中一个长盛不衰的模型，其主要思想是通过迭代训练弱分类器（决策树）以得到最优模型。该模型具有训练效果好、不易过拟合等优点[12]。LightGBM 是一个实现 GBDT 算法的框架，支持高效率的并行训练，并且具有更快的训练速度、更低的内存消耗、更高的准确率、支持分布式、可以快速处理海量数据等优点[12]。LightGBM 集成了多个决策树模型，通过迭代训练来近似最终模型，其基本原理表示为[13]：

$$f(x)=\sum_{t=1}^{N}T(x;\theta_t) \tag{1}$$

式中，$T(x;\theta_t)$ 为单个决策树，N 表示总迭代轮数（决策树个数），θ_t 为决策树参数。

LightGBM 利用直方图算法来寻求最佳分裂点，该算法将连续的特征值划分为 K 个离散的特征后，构造以 K 为宽度的直方图，在遍历数据时，直方图将离散值作为指标积累统计信息，最终根据离散值从直方图中找到最优分割点[14-15]。当使用直方图算法进行计算时，会大大减少信息增益的计算量[16]，因而可以提高计算效率。同时，LightGBM 还利用了 2 种核心算法来降低构建直方图和寻找最优分割点的复杂度，分别是基于梯度的单边采样算法（gradient-based one-side sampling，GOSS）和互斥特征捆绑算法（exclusive feature bundling，EFB），前者可减少样本维度，后者可减少特征维度，使其适用于处理大数据和大量特征问题[17]。

1.2 PSO 算法

PSO 算法是一种进化计算技术，是基于群体智能理论的优化算法，其基本思想是通过群体中个体之间的协作和信息共享来寻找全局最优解，既保留了进化算法的全局搜索策略，又避免了复杂的遗传操作，与进化算法相比是一种更高效的并行搜索算法[18]。虽然 LightGBM 算法在很多方面都表现出良好的效果，但由于其参数众多，且意义多样，参数的不同组合在很大程度上会影响模型的性能，并且参数特点决定了调参工作会十分复杂，极可能落入局部最优的调参范围，而 PSO 算法的全局性与并行性调优特点可以很好地解决这一问题。

PSO 算法假设在 D 维的搜索空间中存在一个由 N 个粒子组成的群体 $X=(X_1,X_2,\cdots,X_N)$，D 即为需要搜索优化的参数个数，粒子 i 可被表示为 D 维向量，其中粒子 i 的位置可表示为：

$$\boldsymbol{X}_i=(\boldsymbol{X}_{i1},\boldsymbol{X}_{i2},\cdots,\boldsymbol{X}_{iD})$$

速度可表示为：

$$\boldsymbol{V}_i=(\boldsymbol{V}_{i1},\boldsymbol{V}_{i2},\cdots,\boldsymbol{V}_{iD})$$

每个粒子都负责维护一个由目标函数决定的适应值（fitness value），并将适应值作为自身移动的根据。为了能够向最优适应值进行“移动”，每个粒子必须掌握 2 项内容：自身经验和群体经验。前者为粒子本身目前为止发现的局部最优位置 $\boldsymbol{P}_{id}$ 和自身所处的位置 $\boldsymbol{X}_i$；后者为目前为止整个群体中所有粒子发现的全局最优位置 $\boldsymbol{P}_{gd}$，全局最优位置是从局部最优位置中得来的，即粒子适应值的局部最优值中的最佳值。粒子在规定的迭代次数或满足规定的误差标准内，在解空间中不断根据个体的局部最优值与群体的全局最优值进行搜索。

在每次迭代中，粒子速度更新的计算公式为：

$$\boldsymbol{V}_{id}^{(t+1)}=\omega\cdot\boldsymbol{V}_{id}^{(t)}+c_1\cdot r_1\cdot(\boldsymbol{P}_{id}^{(t)}-\boldsymbol{X}_{id}^{(t)})+c_2\cdot r_2\cdot(\boldsymbol{P}_{gd}^{(t)}-\boldsymbol{X}_{id}^{(t)}) \tag{2}$$

位置更新的计算公式为：

$$\boldsymbol{X}_{id}^{(t+1)}=\boldsymbol{X}_{id}^{(t)}+\boldsymbol{V}_{id}^{(t)} \tag{3}$$

式（2）～（3）中，ω 是惯性权重；$d=1,2,\cdots,D$；$i=1,2,\cdots,N$；t 为当前迭代数，$\boldsymbol{V}_{id}$ 是粒子 i 的速度矢量，$\boldsymbol{X}_{id}$ 是粒子 i 的位置矢量，$\boldsymbol{P}_{id}$ 是粒子 i 发现的局部最优值，$\boldsymbol{P}_{gd}$ 是全局最优值，c_1、c_2 为学习

因子，r_1、r_2 是介于(0,1)之间的随机数。

粒子群优化算法的流程图如图 1 所示。

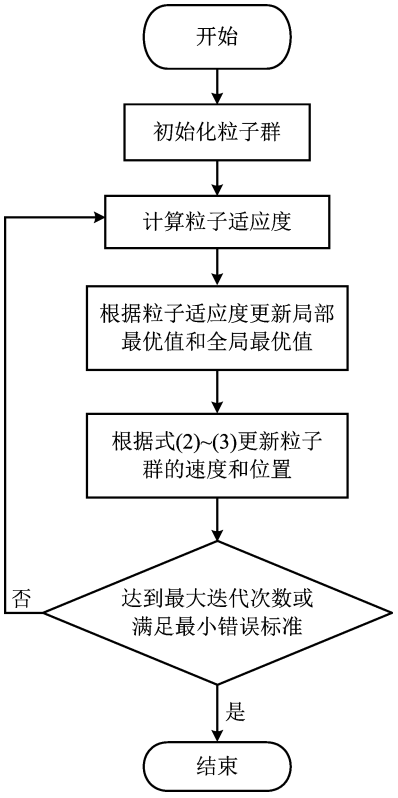


图 1　PSO 算法流程图

Fig. 1　The flow chart of PSO algorithm

1.3　PSO-LightGBM 算法

完整的 LightGBM 参数由核心参数、控制学习过程参数、I/O 参数、目标参数、度量参数、网络参数、GPU 参数和模型参数 8 个模块共 94 个参数组成，其中，核心参数和控制学习过程参数 2 个模块对 LightGBM 性能影响较大，是参数优化研究的重点。由于这 2 个模块共包含了 38 个参数，若对其全部进行优化，会极大地增加计算复杂度，且其中部分参数对于提高模型性能并无明显的助益，因此，为了兼顾模型的训练速度和分类准确率，本文参考 LightGBM 官方文档从核心参数和控制学习过程参数 2 个模块中选取了 8 个主要参数，利用 PSO 算法对其进行优化。各参数信息以及调参结果如表 1 所列。

根据表 1，第 i 个粒子在第 t 次迭代时的速度矢量 $\boldsymbol{V}_i^{(t)}$ 和位置矢量 $\boldsymbol{P}_i^{(t)}$ 可以分别表示为：

$$\begin{aligned}\boldsymbol{V}_i^{(t)}=&[\boldsymbol{V}_{i,\text{learning\_rate}}^{(t)},\boldsymbol{V}_{i,\text{n\_estimators}}^{(t)},\boldsymbol{V}_{i,\text{max\_depth}}^{(t)},\\&\boldsymbol{V}_{i,\text{num\_leaves}}^{(t)},\boldsymbol{V}_{i,\text{feature\_fraction}}^{(t)},\boldsymbol{V}_{i,\text{bagging\_fraction}}^{(t)},\\&\boldsymbol{V}_{i,\text{lambda\_l1}}^{(t)},\boldsymbol{V}_{i,\text{lambda\_l2}}^{(t)}]\end{aligned}\tag{4}$$

$$\begin{aligned}\boldsymbol{P}_i^{(t)}=&[\boldsymbol{P}_{i,\text{learning\_rate}}^{(t)},\boldsymbol{P}_{i,\text{n\_estimators}}^{(t)},\boldsymbol{P}_{i,\text{max\_depth}}^{(t)},\\&\boldsymbol{P}_{i,\text{num\_leaves}}^{(t)},\boldsymbol{P}_{i,\text{feature\_fraction}}^{(t)},\boldsymbol{P}_{i,\text{bagging\_fraction}}^{(t)},\\&\boldsymbol{P}_{i,\text{lambda\_l1}}^{(t)},\boldsymbol{P}_{i,\text{lambda\_l2}}^{(t)}]\end{aligned}\tag{5}$$

表 1　需要优化的参数信息及调参结果

Tab. 1　Parameters to be optimized and the corresponding result

参数	参数内容	调参范围	参数调节主要目的	调参结果
learning_rate	模型训练学习率	[0.001,0.2]	提高模型准确率	0.2
n_estimators	模型训练迭代次数	[100,1 200]	提高模型准确率	1 200
max_depth	树模型最大深度	[3,12]	处理过拟合	12
num_leaves	一棵树上的叶子节点数	(1,1 024)	处理过拟合、提高模型准确率	100
feature_fraction	创建树的特征采样比率	(0.5,1]	处理过拟合、提高训练速度	0.9
bagging_fraction	创建树的数据采样比率	(0.5,1]	处理过拟合、提高训练速度	0.9
lambda_l1	L1 正则化参数	$[10^{-5},3)$	处理过拟合	0.7
lambda_l2	L2 正则化参数	$[10^{-5},3)$	处理过拟合	1

每一轮进化将粒子的位置向量赋给 LightGBM 对应的参数，并根据 LightGBM 模型的分类准确率构造适应度函数来衡量粒子群算法的性能，在 PSO 算法搜索过程中，粒子的适应度越高，则该位置越偏向于最优位置，该参数值越偏向于最优参数值，利用最终得到的最优参数值组合构建 LightGBM 模型，即可得到优化后的分类模型。第 i 个粒子在第 t 次迭代时的适应度函数值表示为：

$$F_i^{(t)}=\frac{1}{n}\sum_{i=1}^{n}(y'_i==y_i)\Big|_{\boldsymbol{P}_i^{(t)}\to\text{LightGBM}}\tag{6}$$

式中，y'_i 为 LightGBM 分类器的预测值，y 为样本

真实标签，n 为样本总数。第 i 个粒子在第 t 次迭代时的局部最优值为：

$$\boldsymbol{P}_{id}^{(t)}=\max(F_i^{(j)}),\quad 0\leqslant j\leqslant t \tag{7}$$

第 i 个粒子在第 t 次迭代时的全局最优值为：

$$\boldsymbol{P}_{gd}^{(t)}=\max(\boldsymbol{P}_{kd}^{(t)}),\quad 1\leqslant k\leqslant N \tag{8}$$

PSO-LightGBM 算法流程如图 2 所示。

2 网络资产脆弱性评估模型

本文基于机器学习方法，构建网络资产的脆弱性评估模型，将网络资产的脆弱性评估任务转化为模型的多分类预测任务。接下来，将从网络资产数据的获取与预处理、网络资产脆弱性评估数据集搭建、模型训练 3 个方面，介绍网络资产脆弱性评估模型的构建过程。方法整体流程图如图 3 所示。

2.1 网络资产数据的获取与预处理

2.1.1 网络资产数据收集

本文通过网络爬虫技术，调用 Censys[18]、Shodan[19]、Fofa[20]以及 360Quake[21]等网络空间测绘系统中的公开接口，收集网络资产数据，并将网络资产的 IP 号和端口号作为其唯一标识以区分不同资产。经过数据清洗，剔除属性信息严重缺失的数据，最终收集到 24 000 条属性信息较为完整的网络资产数据，每条数据包含110维属性，包括 IP、域名、所属行业、所属地区、漏洞信息等。

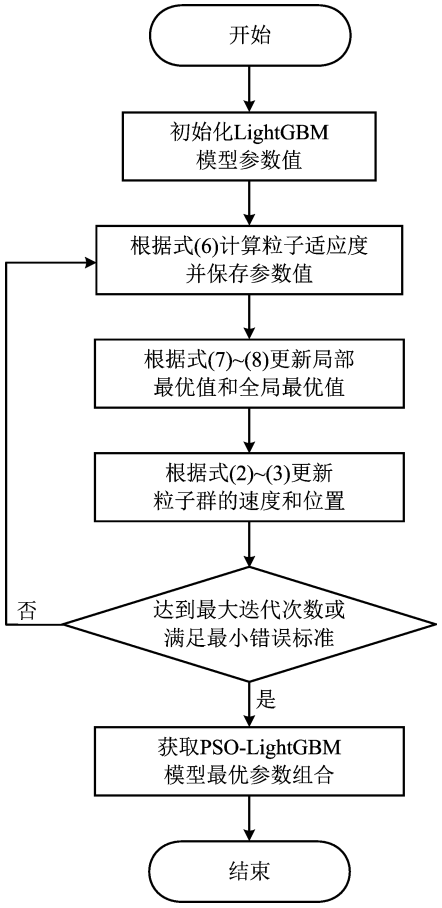


图 2 PSO-LightGBM 算法流程图

Fig. 2 The flow chart of PSO-LightGBM algorithm

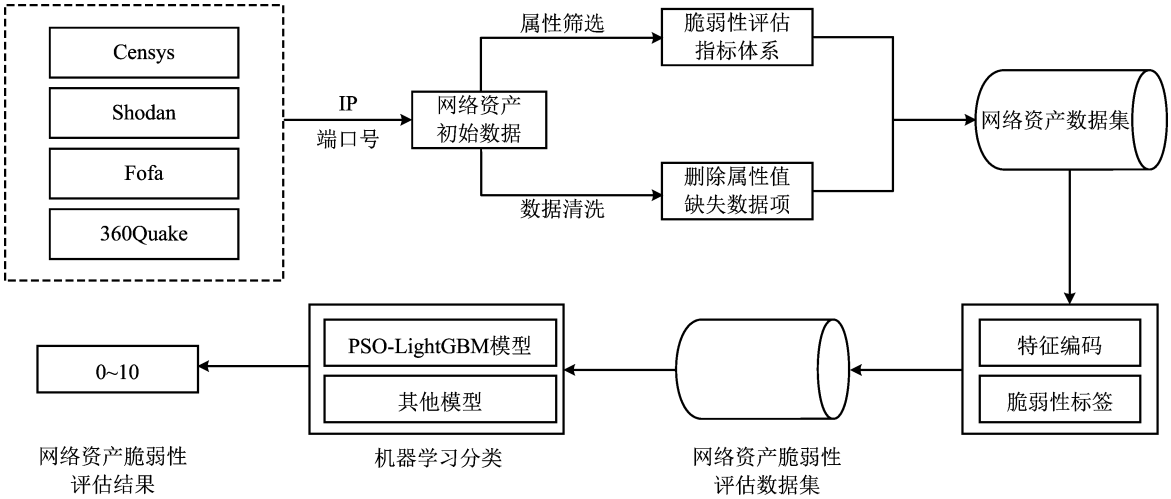


图 3 方法流程图

Fig. 3 The flow chart of the method

2.1.2 网络资产脆弱性评估指标体系

由于收集到的数据在属性上具有高维性和冗余性，难以直接将其全部投入模型进行训练，且部分属性与资产的脆弱性并不存在相关性，因

此，在对数据进行训练之前，首先要明确用于网络资产脆弱性评估的指标，即从众多资产属性中筛选出对资产脆弱性影响较大的属性，并将其作为训练特征。本文参考《电信网和互联网数据安全风险评估实施指南》[22]，结合专家经验，对 110 维网络资产属性进行了合并、筛选，最终确定了 12 个与资产脆弱性相关度最高的属性，并从管理因素、技术因素、漏洞因素 3 个维度，构建用于评估网络资产脆弱性的指标体系，该指标体系的具体内容及其解释说明如表 2 所列，经属性筛选后建立的网络资产数据集包含 24 000 个样本，12 维属性，其部分内容如表 3 所列。

表 2　网络资产脆弱性评估指标体系

Tab. 2　The index system of network assets vulnerability assessment

属性类别	属性名称	标识	说明	实例
管理因素	弱口令	weak_password	是否存在弱口令	不存在
	防火墙	firewall	网络资产是否存在防火墙保护	不存在
	云主机	C_hosting	是否架设在云主机上	否
	CDN	CDN	网络资产是否存在 CDN 技术	不存在
技术因素	操作系统型号	OS	管理计算机硬件与软件资源的计算机程序型号	Ubuntu18
	网站开发语言型号	Lang	网络资产上网站的开发语言	PHP
	Web 容器型号	Web_container	处理从客户端发出请求的服务程序的型号	Apache httpd
	探测到的指纹数量	num_assembly	网络空间测绘系统识别到资产的指纹数量	4
	Web 应用型号	Web_app	一种可以通过 Web 访问的应用程序的型号	WordPress
漏洞因素	漏洞 CVSS 评分	vul_level	资产上存在的经过 POC 验证的漏洞的 CVSS 评分	10
	漏洞编号类型	vul_number	网络资产上存在的经过 POC 验证的漏洞编号所属类型	CVE
	漏洞发现时间	vul_time	网络资产上存在的经过 POC 验证的漏洞发现时间	2022-04-10（1 年内）

表 3　属性筛选后的网络资产数据集

Tab. 3　The network asset data set after attribute filtering

OS	Web_container	Web_app	Num_assembly	Lang	…	Firewall	C_hosting	CDN
CentOS7	Nginx	discuz3	3	PHP	…	存在	是	存在
Ubuntu16	Apache httpd	struts2	2	else	…	不存在	是	不存在
Windows 7	Microsoft IIS httpd7.5	else	else	ASP	…	存在	否	存在
Debian	Java	else	2	JSP	…	存在	否	不存在
else	Apache httpd	Joomla1.5	else	Java	…	不存在	否	存在
FreeBSD	Apache httpd	Joomla1.5	6	Python	…	不存在	否	存在
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

2.2　网络资产脆弱性评估数据集搭建

2.2.1　特征编码

由表 3 可以发现，经属性筛选后的网络资产数据集中，大部分属性值为字符串型数据，不符合机器学习模型对数据特征的数值化要求，因此，在利用机器学习模型对网络资产数据进行训练前，需对这些非数值型属性值进行数值化操作。由于大部分的属性值均可对应离散型数据，为方便模型的训练，在实际进行特征编码之前，本文对数据均进行了统一的离散化处理。

由于 LightGBM 模型本身对数值大小不敏感，属性值数值化后的数值大小对模型不会造成影响，因而本文采用了 Label-Encoding 方法对非数值化的网络资产数据进行数值化操作，按

照某种属性值类型的资产数量在所有资产中所占的比例大小，将其由大到小映射为不同的数值，从而将字符串型属性数据转换为可用于训练的数值特征。以网站开发语言属性为例，本文获取的网络资产数据中，该属性的属性值可以分为 PHP、ASP、JSP、JAVA、Python 及其他语言 6 种情况。其中，采用 PHP 语言的资产数量最多，采用其他语言的次之，采用 Python 语言的最少。按照 Label-Encoding 编码规则，若某资产网站开发语言采用 PHP，则将其属性值置为 0；采用其他语言，则置为 1；采用 ASP，则置为 2；采用 JSP，则置为 3；采用 JAVA，则置为 4；采用 Python，则置为 5。

2.2.2 脆弱性标签

由于经处理后的网络资产数据缺乏脆弱性标签，本文参考 CVSS 评分等级规则，采用专家评分的方法对网络资产数据的脆弱性进行标记，标签值为 0～10，数字由小到大分别表示脆弱性由弱到强。若标签值为 0，则表示当前评估的网络资产非常安全，无脆弱性；反之，若标签值为 10，则表示当前资产脆弱值非常高，具有很高的被攻击风险，需及时对资产进行维护。

为保证标签的正确性，本文的数据集标签均由单一专家评分、专家评分综合、专家复核 3 部分处理后获得。单一专家评分，需将待评分的网络资产数据分发给每一名专家，各位专家依据 2.1 节构建的脆弱性评估指标体系，根据个人经验对每一项资产的脆弱性做出评价。其中，重点参考的因素为管理因素和漏洞因素，因为管理因素主要体现资产是否采取了安全管理的措施，而漏洞因素主要体现资产本身的安全程度，这两者将对资产脆弱性造成直接的影响。以某一资产为例，若检测到该资产不仅存在弱口令，未采用防火墙、云主机等安全管理技术，并且存在漏洞且该漏洞发现时间较长，则认为该资产在未采取安全管理的情况下，其漏洞长时间暴露于网络中，被恶意利用的风险将大大提高，该资产相较于其他不存在漏洞或采取了安全管理措施的资产，将具有更大的脆弱性值。各属性对资产脆弱性的贡献程度，由专家根据个人经验对其进行排序。为避免资产最终的脆弱性评估结果受到个别专家主观评分的影响，还需进行专家评分综合，即将上一步所得的评分结果进行汇总，平均各专家对网络资产脆弱性的不同评分值，获取该资产脆弱性的综合评估值。专家复核，是召集专家对资产脆弱性的综合评估值进行复核，若专家无异议，则通过评估值为该资产的最终脆弱性分值，否则，按照少数服从多数的规则确定该资产的最终脆弱性分值。

综合以上处理步骤，可将表 3 转化为如表 4 所列的网络资产脆弱性评估数据集，该数据集共含有 11 类标签。

表 4 网络资产脆弱性评估数据集

Tab. 4 Data set for vulnerability assessment of network assets

OS	Web_container	Web_app	Num_assembly	Lang	…	Firewall	C_hosting	CDN	Score
0	1	12	3	0	…	1	1	1	5
21	0	4	2	1	…	0	1	0	5
22	13	0	0	2	…	1	0	1	6
11	5	0	2	3	…	1	0	0	1
1	0	3	0	4	…	0	0	1	4
2	0	3	6	5	…	0	0	1	3
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

2.3 机器学习分类

利用 1.3 节介绍的 PSO-LightGBM 模型作为分类器，对网络资产脆弱性值进行多分类预测，分类结果为 0～10。为了验证 PSO-LightGBM 模型在网络资产脆弱性评估上性能的优越性，将该模型与 LightGBM、XGBoost、GBDT、SVM、Naive Bayes 5 种经典机器学习模型在数据集上的表现进行了对比研究，并将 PSO 算法与随机搜索（random search，RS）、贝叶斯优化（Bayesian optimization，BO）这 2 种常用的参数优化算法对 LightGBM 模型的优化效果进行了对比。所有模型的训练与测试均基于 5 次五折交叉验证完成，最终每个模型的评估指标值取该模型测试结果的平均值。

3　实验结果与分析

本节对基于 PSO-LightGBM 的网络资产脆弱性评估模型的效果进行了展示，并对 PSO-LightGBM 模型与其他机器学习模型的对比结果进行了分析讨论。

3.1　评估指标

利用准确率、精确率、召回率、F_1-score 4 种用于评价分类模型性能的指标，来评价网络资产脆弱性评估模型的表现。评估结果可分为 4 类，即真正例(true positive，TP)、假正例(false positive，FP)、真反例(true negative，TN)和假反例(false negtive，FN)。T_{TP} 为模型将正例预测正确的个数，即样本为正例，模型预测为正例；F_{FP} 为模型将反例预测错误的个数，即样本为反例，模型预测为正例；T_{TN} 为模型将反例预测正确的个数，即样本为反例，模型预测为反例；F_{FN} 为模型将正例预测错误的个数，即样本为正例，模型预测为反例。

准确率是模型对资产评分的正确预测数量与总数据集数量的比率，其计算公式为：

$$A_{\text{Accuracy}}=\frac{T_{TP}+T_{TN}}{T_{TP}+T_{TN}+F_{FP}+F_{FN}} \tag{9}$$

精确率是模型正确预测的正例数量与所有预测为正例的数量之比，其计算公式为：

$$P_{\text{Precision}}=\frac{T_{TP}}{T_{TP}+F_{FP}} \tag{10}$$

召回率是模型正确预测的正例数量与所有真实正例数量之比，其计算公式为：

$$R_{\text{Recall}}=\frac{T_{TP}}{T_{TP}+F_{FN}} \tag{11}$$

F_1-score 为准确率与精确率的加权平均值，其计算公式为：

$$F_1=\frac{2\cdot P_{\text{Precision}}\cdot R_{\text{Recall}}}{P_{\text{Precision}}+R_{\text{Recall}}} \tag{12}$$

3.2　实验结果

利用 PSO-LightGBM 模型对网络资产脆弱性进行分类的各项评估指标值如表 5 所列。从表中可以看出，该模型在网络资产脆弱性多分类问题上的平均准确率、精确率、召回率、F_1-score 均在 91%以上，具有较好的分类效果。

表 5　PSO-LightGBM 模型评估指标值

Tab. 5　Evaluation indicator values of PSO-LightGBM model

(%)

准确率	精确率	召回率	F_1-score
91.24	91.23	91.24	91.24

利用 PSO-LightGBM 模型对网络资产脆弱性进行分类预测的平均结果集如表 6 所列，可视化后的平均混淆矩阵如图 4 所示，从分类结果可以看出，本文提出的网络资产脆弱性分类模型并未出现过拟合的现象。此外，由于在数据集在脆弱性等级为 0 和 10 上的数据较多，所以对于 0 类和 10 类的数据，模型表现出较高的测试准确率；相反，在脆弱性等级为 6、7 和 8 上的数据较少，模型在这些类上的测试准确率相对较低。综合表 5 和图 4 可以看出，PSO-LightGBM 模型在网络资产脆弱性数据集上的各评估指标均表现良好，因此，该模型可对各脆弱性等级的网络资产数据进行精确分类。

表 6　PSO-LightGBM 模型的平均结果集

Tab. 6　The average result set of PSO-LightGBM model

脆弱性等级	0	1	2	3	4	5	6	7	8	9	10
正确预测	626	347	473	467	413	316	212	173	169	279	908
错误预测	18	48	24	35	44	44	56	41	51	42	18
正确率(%)	97.2	87.8	95.2	93.0	90.4	87.8	79.1	80.8	76.8	86.9	98.1
错误率(%)	2.8	12.2	4.8	7.0	9.6	12.2	20.9	19.2	23.2	13.1	1.9

3.3　不同模型/算法对比

PSO-LightGBM 模型与其他机器学习模型在网络资产脆弱性评估数据集上的性能对比如表 7 所列。由表 7 可以看出，PSO-LightGBM 模型相较于其他模型在准确率、精确率、召回率、F_1-score 上均表现最优。

为了更直观地展示各模型在准确率、精确率、召回率、F_1-score 4 项指标上的表现情况，绘制各模型指标值对比，如图 5 所示。

PSO 算法与随机搜索法、贝叶斯优化算法在

LightGBM 模型参数优化上的效果对比如表 8 所示。可以观察出，虽然随机搜索法和贝叶斯优化算法均在优化 LightGBM 模型上具有一定的效果，但显然 PSO 算法比另外 2 种算法更有优势。

表 7 不同模型评估指标值对比

Tab. 7 Comparison of the evaluation index values of different models (%)

模型	准确率	精确率	召回率	F_1-score
PSO-LightGBM	91.24	91.23	91.24	91.24
LightGBM	89.04	89.03	89.03	89.04
XGBoost	67.21	67.20	67.20	67.20
GBDT	57.64	57.62	57.62	57.64
SVM	54.50	54.50	54.49	54.50
Naive Bayes	46.20	46.19	46.19	46.19

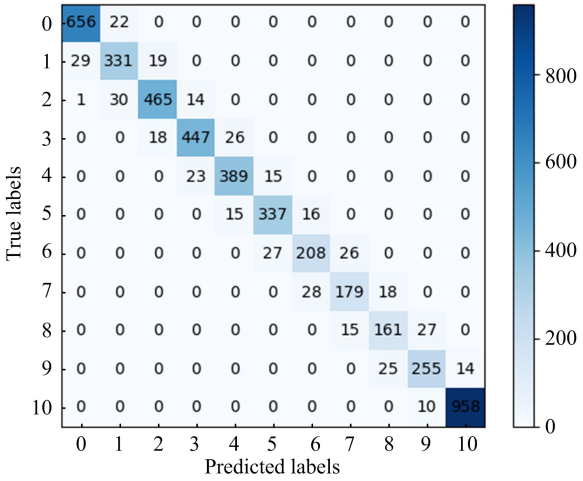
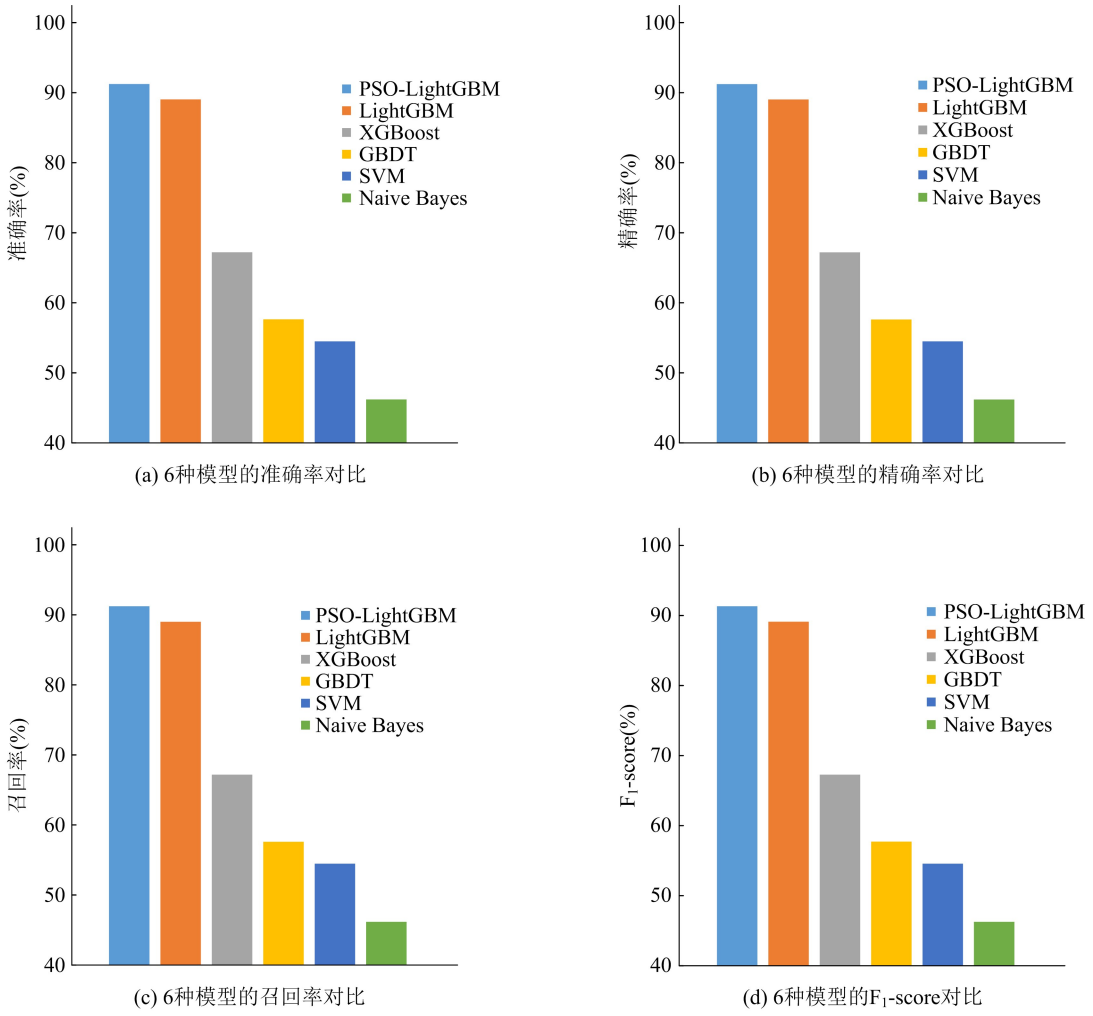


图 4 PSO-LightGBM 模型平均混淆矩阵

Fig. 4 The average confusion matrix of PSO-LightGBM model



(a) 6种模型的准确率对比

(b) 6种模型的精确率对比

(c) 6种模型的召回率对比

(d) 6种模型的F_1-score对比

图 5 6 种模型的指标对比

Fig. 5 Comparison of indicators of six models

表 8　不同优化算法效果对比

Tab. 8　Effect comparison of different optimization algorithms

(%)

优化算法(+LightGBM)	准确率	精确率	召回率	F_1-score
PSO-LightGBM	91.24	91.23	91.24	91.24
RS-LightGBM	89.56	89.55	89.56	89.56
BO-LightGBM	91.02	91.01	91.02	91.01

从图 5 可以看出，Naive Bayes 模型和 SVM 模型的准确率、精确率、召回率和 F_1-score 在 6 种算法中是最低的，这是由于 Naive Bayes 算法只有在各属性特征间相互独立的条件下，才能表现出其良好的分类性能，经分析属性间的相关性发现，网络资产脆弱性数据集中的 12 个属性特征中有部分属性间存在着较强的相关性；而 SVM 本身是一种二分类器，对于网络资产脆弱性分类这种 11 分类问题，并不能取得较好的效果。因此，Naive Bayes 模型和 SVM 模型并不适合作为网络资产的脆弱性分类模型。由于 XGBoost 算法是在 GBDT 的基础上对 Boosting 算法进行的改进，它的表现略优于 GBDT，而 LightGBM 相对于 XGBoost 在框架上进行了优化，采用了 GOSS 和 EFB 2 种新技术，防止了过拟合，减少了特征的数量，因此它的性能相较于除 PSO-LightGBM 以外的其他 3 种方法最佳。从表 8 可以看出，PSO 算法相对于随机搜索法和贝叶斯优化算法具有更大的优势。随机搜索法由于其随机采样的参数更新方式，往往容易遗失重要信息，导致其表现不佳，贝叶斯优化在测试新的采样点时会充分考虑上一个点的信息，从而改进了随机搜索的缺陷，但容易陷入局部最优，而由于 PSO 算法维护局部最优值和全局最优值 2 个变量的特点，往往更不易陷入局部最优的情况。通过实验对比可以验证，本文所利用的 PSO-LightGBM 模型在准确率、精确率、召回率、F_1-score 4 项指标中均表现最优，这说明采用粒子群算法进行模型参数优化的 LightGBM 模型，在网络资产脆弱性分类上具有最佳效果。因此粒子群算法可以有效优化 LightGBM 的参数，提高对数据集的分类准确率。从模型综合分类表现的角度来看，采用 PSO-LightGBM 模型进行网络空间资产的脆弱性评估比其他模型和算法更合理。

3.4　讨论与分析

LightGBM 模型是近年来深受关注的机器学习模型，也是目前机器学习领域性能最佳的模型之一，本文通过实验验证，该模型可以实现网络资产脆弱性等级的准确分类，准确率可以达到 91%以上，该结果也是目前为止在相关研究中取得的最高准确率。由于 LightGBM 模型参数较为复杂，导致其调参维度高且极可能落入局部最优的调参范围，而 PSO 算法可以很好地适配 LightGBM 模型的调参特点，能够自动收集全局范围内的空间信息，具有很好的全局性和并行性，通过实验验证了其良好的模型提升效果。为了进一步说明本文所提出的网络资产脆弱性评估方法对数据集以外数据的适用性，本文以新爬取的 2 条网络资产数据(资产 A、B)为例，采用 2.1 与 2.2 节中所列的数据预处理方法对其进行处理后，利用网络资产脆弱性评估模型对其进行脆弱性评估，处理后的网络资产数据及其评估结果如表 9 所列。评估结果显示，B 资产脆弱性等级为 4，相对于 A 资产存在着更高的脆弱性，说明对于 B 资产存在更高的风险，需要及时施加安全维护措施以及时修复其脆弱性。通过观察可以发现，2 个资产之间属性的主要差别在于 B 资产存在着明显高于 A 资产的漏洞评分，以及相对较弱的安全管理措施(未设置防火墙)，因而导致了其脆弱性程度较高，该评估结果符合常理。

表 9　新爬取的网络资产数据脆弱性评估结果

Tab. 9　Vulnerability assessment results of newly crawled network asset data

资产	OS	Web_container	Web_app	Num_assembly	vul_number	vul_level	vul_time	Lang	weak_password	firewall	C_hosting	CDN	score
A	Ubuntu14	else	wordpress5	2	QVE	2	1 天内	else	0	1	1	1	1
B	Ubuntu 20	else	openresty1.14	2	QVE	5	1 天内	else	0	0	1	1	4

4　结束语

网络空间资产脆弱性评估，对保护脆弱资产、降低资产被攻击风险、预防网络安全事故具有重要意义，然而，目前该方面的研究还比较匮乏。为此，本文提出了一种针对网络空间资产的

脆弱性评估方法。首先,依据行业标准和专家经验,提出网络资产脆弱性评估指标体系,并基于真实的网络资产数据,建立网络资产脆弱性评估数据集;其次,将 LightGBM 机器学习模型和 PSO 算法结合,构建基于 PSO-LightGBM 的网络资产脆弱性评估模型,实现网络资产脆弱性的自动评估;最后,将 PSO-LightGBM 模型与其他机器学习学习模型在数据集上的表现进行对比分析,验证该模型对网络资产脆弱性评估的有效性。实验结果表明,PSO-LightGBM 模型在网络资产脆弱性评估问题上具有优于其他模型的表现,本文提出的方法可实现对网络资产脆弱性的准确评估。

虽然本文提出的方法对网络资产的脆弱性评估取得了较好的效果,但值得注意的是,该方法仍然存在局限性。本方法基于构建的脆弱性评估指标体系以及数据预处理方法,采用机器学习的方法实现脆弱性的分类预测,利用该方法的基本前提是用于评估的数据属性相对于评估指标是完整的,对于无法通过爬取获得相关属性的资产将无法采用本方法进行脆弱性评估,虽然用于模型训练的数据均具备属性完整性,但在数据采集阶段部分缺失属性的数据已被排除在外,在一定程度上会影响该方法的普适性,未来研究工作中,应探索实现缺失属性数据补全的方法,并将其与资产的脆弱性评估结合起来,以进一步提高数据集的代表性。此外,由于脆弱性评估属于多分类问题,标签的划分范围较大(0~10)且各类别间数据量存在不均衡问题,不可避免地会对模型的分类效果造成一定影响,本文的方法虽然可以实现 91%的分类准确率,但仍然存在较大的提升空间,未来可继续挖掘适用于解决多分类问题的新方法,并解决数据的不均衡问题,进一步提高脆弱性评估的准确率。

参 考 文 献

[1] 邓晓晖,李伟辰,曹文杰. 基于测绘技术的网络资产安全管理研究[J].保密科学技术,2021(3):36-40.
DENG Xiaohui, LI Weichen, CAO Wenjie. Research on network asset security management based on surveying and mapping technology [J]. Secrecy Science and Technology, 2021(3): 36-40. (in Chinese)

[2] 赵帆,罗向阳,刘粉林. 网络空间测绘技术研究[J]. 网络与信息安全学报,2016,2(9):1-11.
ZHAO Fan, LUO Xiangyang, LIU Fenlin. Research on cyberspace surveying and mapping technology[J]. Chinese Journal of Network and Information Security, 2016, 2(9): 1-11. (in Chinese)

[3] 史光庭,阮文波. 网络空间测绘技术的应用研究[J]. 保密科学技术,2021(3):20-28.
SHI Guangting, RUAN Wenbo. Research on the application of cyberspace mapping technology[J]. Secrecy Science and Technology, 2021(3): 20-28. (in Chinese)

[4] ELBAZ C, RILLING L, MORIN C. Fighting N-day vulnerabilities with automated CVSS vector prediction at disclosure[C]//Proceedings of the 15th International Conference on Availability, Reliability and Security. NY: ACM, 2020: 1-10.

[5] 周诗洋,傅鹏. CVSS 环境指标变量对系统安全的影响研究[J]. 计算机工程与科学,2016,38(12):2463-2470.
ZHOU Shiyang, FU Li. Influence of CVSS environmental metrics on system security[J]. Computer Engineering & Science, 2016, 38(12): 2463-2470. (in Chinese)

[6] JIANG Y, ATIF Y. Towards automatic discovery and assessment of vulnerability severity in cyber-physical systems[J]. Array, 2022, 15: 100209.

[7] LI X T, LI H, SUN B Z, et al. Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA[J]. Journal of Intelligent & Fuzzy Systems, 2018, 34: 2491-2501.

[8] XIONG J X, WU J Z. Construction of information network vulnerability threat assessment model for CPS risk assessment [J]. Computer Communications, 2020, 155: 197-204.

[9] 游梦娜. 基于攻击图的网络脆弱性评估技术研究与实现[D]. 北京:北京邮电大学,2018.
YOU Mengna. Research and implementation of network vulnerability assessment technology based on attack graph[D]. Beijing: Beijing University of Posts and Telecommunications, 2018. (in Chinese)

[10] 黄波,秦玉海,刘旸,等. 基于通用攻击树的脆弱性评估与风险概率研究[J]. 信息网络安全,2022,22(10):39-44.
HUANG Bo, QIN Yuhai, LIU Yang, et al. Research of vulnerability assessment and risk probability base on general attack tree [J]. Netinfo Security, 2022, 22(10): 39-44. (in Chinese)

[11] YANG H, FENG Y. Fuzzy Petri nets based information system security situation assessment model[C]//Proceedings of International Conference on Foundations of Computer Science. Singapore: Springer,

2020：283-293.

[12] 吴琼，李荣琳，洪海生，等. 基于混合重抽样和 LightGBM 算法的配变低压跳闸预测[J]. 电力系统保护与控制，2021，49(12)：71-78.
WU Qiong，LI Ronglin，HONG Haisheng，et al. Low-voltage tripping prediction of a distribution transformer based on hybrid resampling and a LightGBM algorithm[J]. Power System Protection and Control，2021，49(12)：71-78.(in Chinese)

[13] LI M. Bike-sharing demand prediction model based on PSO-lightgbm algorithm[C]//Proceedings of the 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). Chongqing：IEEE，2022：2080-2085.

[14] SUN T，WANG Y，JIN X，et al. Multi-station joint forecast model of water level in Hongze lake based on PSO-LightGBM [C]//Proceedings of the 7th International Conference on Hydraulic and Civil Engineering & Smart Water Conservancy and Intelligent Disaster Reduction Forum (ICHCE & SWIDR). Nanjing：IEEE，2021：152-159.

[15] GARCIA-ARROYO J L. Segmentation of skin lesions in dermoscopy images using fuzzy classification of pixels and histogram thresholding [J]. Computer Methods and Programs in Biomedicine，2019，168：11-19.

[16] 丁建立，孙玥. 基于 LightGBM 的航班延误多分类预测[J]. 南京航空航天大学学报，2021，53(6)：847-854.
DING Jianli，SUN Yue. Multi-classification prediction of flight delay based on LightGBM[J]. Journal of Nanjing University of Aeronautics and Astronautics，2021，53(6)：847-854.(in Chinese)

[17] KE G L，QI M，FINLEY T，et al. LightGBM：a highly efficient gradient boosting decision tree[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. NY：Curran Associates Inc，2017：3149-3157.

[18] 2023 CENSYS. The Censys platform[EB/OL].[2023-01-12]. https://www.censys.io/.

[19] SHODAN. Search engine for the Internet of everything [EB/OL]. [2023-01-12]. https://www.shodan.io/.

[20] 华顺信安. Fofa 网络空间测绘[EB/OL].[2023-01-12]. https://fofa.so/.

[21] 三六零数字安全集团. 360Quake[EB/OL].[2023-01-12]. https://quake.360.net/quake/.

[22] 信息产业部电信研究院. 电信网和互联网数据安全风险评估实施指南[S]. 北京：中华人民共和国信息产业部，2008.

作 者 简 介

王晨巍
女，1999 年生，硕士研究生，研究方向为网络安全
E-mail：ChenWeiWang@mail.hfut.edu.cn

黎歆雨
女，1999 年生，硕士研究生，研究方向为网络安全
E-mail：xinyuli@mail.hfut.edu.cn

高大伟
男，1981 年生，审计师，研究方向为大数据审计
E-mail：17666191@qq.com

沈　毅
男，1985 年生，副教授，研究方向为网络空间安全
E-mail：shenyi@nudt.edu.cn

李　萌
男，1988 年生，博士，副研究员，研究方向为车联网隐私保护、车联网隐私度量、车联网隐私挖掘
E-mail：mengli@hfut.edu.cn

责任编辑　董　莉