

# 信息安全学报

Journal of Cyber Security

第 8 卷 第 3 期 2023 年 5 月

## 目 次

基于特征分布差异的对抗样本检测 .....	1
韩 蒙, 俞伟平, 周依云, 杜文涛, 孙彦斌, 林昶廷	
基于健壮半径求解的循环神经网络形式化验证方法 .....	12
赵 亮, 戚润川, 段鑫民, 李春奕, 王小兵	
基于分治法的神经网络修复方法 .....	27
孙 朔, 严 俊, 晏荣杰	
基于 BFV 同态加密神经网络参数设置实证研究 .....	38
杨 涛, 董建锋	
保护用户数量信息的安全虹膜识别方案 .....	49
周 宇, 向剑文, 郑倩荣, 赵冬冬	
基于深度学习的跨自然语言与程序语言生成任务综述 .....	65
宋小祎, 张若定, 张 妍, 张梅山, 黎家通	
基于模型驱动的分治并行函数式程序生成及自动验证 .....	85
王昌晶, 王忠文, 潘 丞, 黄 箐, 左正康	
IoT 设备程序同源性智能检测技术综述 .....	103
孔凯薇, 霍冬冬, 苏东楠, 徐 震	
基于联邦学习的第三方库流量识别 .....	128
崔华俊, 孟国柱, 李玥琦, 张 棣, 代玥玥, 杨慧然, 朱大立, 王伟平	

# Journal of Cyber Security

Volume 8    Issue 3    May, 2023

## Contents

Exploiting Feature Space Divergence For Adversarial Example Detection .....	1
<i>HAN Meng, YU Weiping, ZHOU Yiyun, DU Wentao, SUN Yanbin, LIN Changting</i>	
A Formal Verification Method for Recurrent Neural Network Based on Robustness Radius Solving .....	12
<i>ZHAO Liang, QI Runchuan, DUAN Xinmin, LI Chunyi, WANG Xiaobing</i>	
A Neural Network Repair Method Based on Divide-and-Conquer .....	27
<i>SUN Shuo, YAN Jun, YAN Rongjie</i>	
Empirical Study on the effects of BFV Scheme Configuration on Secure Neural Networks Inference .....	38
<i>YANG Tao, DONG Jianfeng</i>	
Secure Iris Recognition with the Protection of the Number of Users .....	49
<i>ZHOU Yu, XIANG Jianwen, ZHENG Qianrong, ZHAO Dongdong</i>	
A Review of Deep Learning Based Generation Tasks Across Natural and Programming Languages .....	65
<i>SONG Xiaoyi, ZHANG Ruoding, ZHANG Yan, ZHANG Meishan, LI Jiatong</i>	
Model-driven Divide-and-conquer Parallel Functional Program Generation and Automatic Verification .....	85
<i>WANG Changjing, WANG Zhongwen, PAN Cheng, HUANG qing, ZUO Zhengkang</i>	
Survey of Intelligent Homology Detection Technology for IoT Programs .....	103
<i>Kong Kaiwei, Huo Dongdong, Su Dongnan, Xu Zhen</i>	
A Third-party Library Traffic Identification Framework Using Federated Learning .....	128
<i>Cui Huajun, Meng Guozhu, Li Yueqi, Zhang yan, Dai Yueyue, Yang Huiran, Zhu Dali, Wang Weiping</i>	