第8卷 | 第3期 | Vol.8 | No.3 May 2023

ISSN 2096-1146
CN10-1380/TN

信息安全学报 Journal of Cyber Security 2023年5月 May 2023 科学出版社

信息安全学报

Journal of Cyber Security

中国计算机学会会刊
计算机学会推荐中文期刊（B类）
通信学会推荐中文期刊（B类）
Scopus收录期刊
CSCD收录期刊
中国科技核心期刊

ISSN 2096-1146

主办 中国科学院信息工程研究所 INSTITUTE OF INFORMATION ENGINEERING,CAS
SKLOIS 信息安全国家重点实验室
科学出版社 Science Press

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　棪, 代玥玥, 杨慧然, 朱大立, 王伟平

期刊基本参数：CN 10-1380/TN * 2016 * b * 16 * 156 * zh * P * ￥60 * 2000 * 10 * 2023-03

Journal of Cyber Security

Volume 8 Issue 3 May, 2023

Contents

Exploiting Feature Space Divergence For Adversarial Example Detection ····· 1
HAN Meng, YU Weiping, ZHOU Yiyun, DU Wentao, SUN Yanbin, LIN Changting

A Formal Verification Method for Recurrent Neural Network Based on Robustness Radius Solving ····· 12
ZHAO Liang, QI Runchuan, DUAN Xinmin, LI Chunyi, WANG Xiaobing

A Neural Network Repair Method Based on Divide-and-Conquer ····· 27
SUN Shuo, YAN Jun, YAN Rongjie

Empirical Study on the effects of BFV Scheme Configuration on Secure Neural Networks Inference ····· 38
YANG Tao, DONG Jianfeng

Secure Iris Recognition with the Protection of the Number of Users ····· 49
ZHOU Yu, XIANG Jianwen, ZHENG Qianrong, ZHAO Dongdong

A Review of Deep Learning Based Generation Tasks Across Natural and Programming Languages ····· 65
SONG Xiaoyi, ZHANG Ruoding, ZHANG Yan, ZHANG Meishan, LI Jiatong

Model-driven Divide-and-conquer Parallel Functional Program Generation and Automatic Verification ····· 85
WANG Changjing, WANG Zhongwen, PAN Cheng, HUANG qing, ZUO Zhengkang

Survey of Intelligent Homology Detection Technology for IoT Programs ····· 103
Kong Kaiwei, Huo Dongdong, Su Dongnan, Xu Zhen

A Third-party Library Traffic Identification Framework Using Federated Learning ····· 128
Cui Huajun, Meng Guozhu, Li Yueqi, Zhang yan, Dai Yueyue, Yang Huiran, Zhu Dali, Wang Weiping

信息安全学报

Xinxi Anquan Xuebao

（双月刊，2016年创刊）

第8卷 第3期 2023年5月

Journal of Cyber Security

（Bimonthly）

（Started in 2016）

Vol.8 No.3 May 2023

编　　辑　《信息安全学报》编辑部
（北京海淀区树村路19号，
邮编 100085）
电话：010-82345198 010-82345199
E-mail：jcs@iie.ac.cn

主　　编　方滨兴

主办单位　中国科学院信息工程研究所
中国科技出版传媒股份有限公司

主管单位　中国科学院

出　　版　中国科技出版传媒股份有限公司

印刷装订　北京科信印刷有限公司

总 发 行　中国科技出版传媒股份有限公司
地址：北京东黄城根北街16号
邮政编码：100717
电话：010-64017032
E-mail:journal@mail.sciencep.com

Edited by Editorial Board of Journal of Cyber Security
(No.19 Shucun Road, Haidian District, Beijing
100085, China)
E-mail: jcs@iie.ac.cn
Editor-in-Chief: Binxing Fang
Sponsored by Institute of Information Engineering,
Chinese Academy of Sciences(IIECAS);
China Science Publishing & Media LTD
Published by China Science Publishing & Media LTD
Printed by Beijing Kexin Printing Limited Company
Distributed by Science Press
No.16 Donghuangchenggen North Street
Beijing 100717,China
Telephone:010-64017032
E-mail:journal@mail.sciencep.com

刊号：ISSN 2096-1146
CN10-1380/TN

公 开 发 行

邮发代号：80-601

定价：60.00元