

计算机研究与发展

第五十九卷

第十期

二〇二二年十月

科学出版社



ISSN 1000-1239
CODEN JYYFEY

Journal of Computer Research and Development

计算机研究与发展

第 59 卷 第 10 期 2022 年 10 月
Vol. 59 No. 10 Oct. 2022

主办 中国科学院计算技术研究所 中国计算机学会 出版 科学出版社



中国计算机学会会刊



目次

数据安全与智能隐私保护研究专题

前言 曹珍富 徐秋亮 张玉清 董晓蕾 (2101)

综 述

云边端全场景下深度学习模型对抗攻击和防御 李 前 蔺琛皓 杨雨龙 沈 超 方黎明 (2109)

基于通用数据保护条例的数据隐私安全综述
..... 赵景欣 岳星辉 冯崇朋 张 静 李 印 王 娜 任家东 张昊星 伍高飞 朱笑岩 张玉清 (2130)

面向图像分类的对抗鲁棒性评估综述 李自拓 孙建彬 杨克巍 熊德辉 (2164)

物联网访问控制安全性综述 刘奇旭 靳 泽 陈灿华 高新博 郑宁军 方仪伟 冯 云 (2190)

数据安全

区块链群智感知中基于隐私数据真值估计的激励机制 应臣浩 夏福源 李 颀 斯雪明 骆 源 (2212)

多因素反向拍卖的跨链支付路由方案 张 谦 曹 晟 张小松 (2233)

支持密钥更新与审计者更换的云安全审计方案 周 磊 陈珍珠 付安民 苏 铨 俞 研 (2247)

效用优化的本地差分隐私集合数据频率估计机制 曹依然 朱友文 贺星宇 张 跃 (2261)

uBlock 类结构最优向量置换的高效搜索 李晓丹 吴文玲 张 丽 (2275)

高效且恶意安全的三方小集合隐私交集计算协议 张 蕾 贺崇德 魏立斐 (2286)

基于 MILP 寻找 SM4 算法的差分特征 潘印雪 王高丽 倪建强 (2299)

一种支持联合搜索的多用户动态对称可搜索加密方案 张蓝蓝 曹卫东 王怀超 (2309)

智能隐私保护

基于神经元激活模式控制的深度学习训练数据泄露诱导 潘旭东 张 谥 杨 珉 (2323)

基于秘密分享的高效隐私保护四方机器学习方案 阎允雪 马 铭 蒋 瀚 (2338)

基于边缘样本的智能网络入侵检测系统数据污染防御方法 刘广睿 张伟哲 李欣洁 (2348)

一种嵌入式 Linux 系统上的新型完整性度量架构 贾巧雯 马昊玉 厉 严 王哲宇 石文昌 (2362)

编者专栏

《计算机研究与发展》征订启事 (2274)

《计算机研究与发展》2020 年论文高被引 TOP10 (2376)

《计算机研究与发展》编委会 (封底)

责任编辑:沈宝丽 互校编辑:黄冠华

JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT

Vol. 59 No. 10 October 2022

CONTENTS

Special Issue on Data Security and Intelligent Privacy Preserving

Preface Cao Zhenfu , et al. (2101)

Survey

Adversarial Attacks and Defenses Against Deep Learning Under the Cloud-Edge-Terminal Scenes
..... Li Qian , et al. (2109)

Survey of Data Privacy Security Based on General Data Protection Regulation Zhao Jingxin , et al. (2130)

A Review of Adversarial Robustness Evaluation for Image Classification Li Zituo , et al. (2164)

Survey on Internet of Things Access Control Security Liu Qixu , et al. (2190)

Data Security

Incentive Mechanism Based on Truth Estimation of Private Data for Blockchain-Based Mobile
Crowdsensing Ying Chenhao , et al. (2212)

A Multi-Factor Reverse Auction Routing Scheme for Cross-Blockchain Payment Zhang Qian , et al. (2233)

Cloud Secure Auditing Scheme Supporting Key Update and Auditor Replacement Zhou Lei , et al. (2247)

Utility-Optimized Local Differential Privacy Set-Valued Data Frequency Estimation Mechanism
..... Cao Yiran , et al. (2261)

Efficient Search for Optimal Vector Permutations of uBlock-like Structures Li Xiaodan , et al. (2275)

Efficient and Malicious Secure Three-Party Private Set Intersection Computation Protocols for
Small Sets Zhang Lei , et al. (2286)

Finding Differential Characteristics of SM4 Algorithm Based on MILP Pan Yinxue , et al. (2299)

A Multi-User Dynamic Symmetric Searchable Encryption Scheme Supporting Conjunctive Search
..... Zhang Lanlan , et al. (2309)

Intelligent Privacy Preserving

Fishing Leakage of Deep Learning Training Data via Neuron Activation Pattern Manipulation ...
..... Pan Xudong , et al. (2323)

An Efficient Privacy Preserving 4PC Machine Learning Scheme Based on Secret Sharing Yan Yunxue , et al. (2338)

Data Contamination Defense Method for Intelligent Network Intrusion Detection Systems Based
on Edge Examples Liu Guangrui , et al. (2348)

A Novel Integrity Measurement Architecture for Embedded Linux Systems Jia Qiaowen , et al. (2362)

Editorial Columns (2274,2376,back cover)

《计算机研究与发展》第九届编委会

The 9th Editorial Board of Journal of Computer Research and Development

主 编	Editor-in-Chief
	徐志伟 Xu Zhiwei
副 主 编	Associate Editors-in-Chief
	郑纬民 Zheng Weimin 吕 建 Lü Jian 钱德沛 Qian Depei
	冯登国 Feng Dengguo 周志华 Zhou Zhihua
荣誉编委	Honorary Editors
	石纯一 Shi Chunyi 史忠植 Shi Zhongzhi 陈国良 Chen Guoliang
领域编委	Leading Editors
	李华伟(体系结构) Li Huawei (Computer Architecture)
	马华东(网络技术) Ma Huadong (Network Technology)
	陈恩红(人工智能) Chen Enhong (Artificial Intelligence)
	秦志光(信息安全) Qin Zhiguang (Information Security)
	李宣东(软件技术) Li Xuandong (Software Technology)
	金海(并行与分布式计算) Jin Hai (Parallel and Distributed Computing)
	彭宇新(应用技术) Peng Yuxin (Application Technology)

编 委 Editors

曹军威 Cao Junwei	曹珍富 Cao Zhenfu	曹子宁 Cao Zining
车武军 Che Wujun	陈海波 Chen Haibo	陈 昕 Chen Xin
陈云霄 Chen Yunji	陈左宁 Chen Zuoning	崔 莉 Cui Li
窦 勇 Dou Yong	方滨兴 Fang Binxing	冯志勇 Feng Zhiyong
高云君 Gao Yunjun	过敏意 Guo Minyi	侯丽珊 Hou Lishan
侯 锐 Hou Rui	黄 华 Huang Hua	黄刘生 Huang Liusheng
黄萱菁 Huang Xuanjing	蒋树强 Jiang Shuqiang	金澈清 Jin Cheqing
李肯立 Li Kenli	李仁发 Li Renfa	梁吉业 Liang Jiye
廖士中 Liao Shizhong	林 闯 Lin Chuang	刘国华 Liu Guohua
刘 杰 Liu Jie	刘 挺 Liu Ting	刘志勇 Liu Zhiyong
罗军舟 Luo Junzhou	吕建成 Lü Jiancheng	马晓星 Ma Xiaoxing
梅 宏 Mei Hong	孟祥旭 Meng Xiangxu	孟小峰 Meng Xiaofeng
苗奇谦 Miao Duoqian	欧阳丹彤 Ouyang Dantong	任丰原 Ren Fengyuan
舒继武 Shu Jiwu	孙茂松 Sun Maosong	孙晓明 Sun Xiaoming
陶建华 Tao Jianhua	王兴伟 Wang Xingwei	王意洁 Wang Yijie
王永吉 Wang Yongji	吴 飞 Wu Fei	谢高岗 Xie Gaogang
徐明伟 Xu Mingwei	徐秋亮 Xu Qiuliang	薛向阳 Xue Xiangyang
杨 博 Yang Bo	杨学军 Yang Xuejun	于 戈 Yu Ge
于 剑 Yu Jian	詹乃军 Zhan Naijun	张广艳 Zhang Guangyan
张敏灵 Zhang Minling	张 伟 Zhang Wei	张悠慧 Zhang Youhui
张玉清 Zhang Yuqing	章 毅 Zhang Yi	赵险峰 Zhao Xianfeng
郑庆华 Zheng Qinghua	周傲英 Zhou Aoying	周 昆 Zhou Kun
祝烈煌 Zhu Liehuang		

青年编委 Youth Editors

陈 恺 Chen Kai	郭嘉丰 Guo Jiafeng	何 源 He Yuan
李宇峰 Li Yufeng	李振宇 Li Zhenyu	刘知远 Liu Zhiyuan
彭 鑫 Peng Xin	屈龙江 Qu Longjiang	熊 虎 Xiong Hu
许长桥 Xu Changqiao	严 严 Yan Yan	张 蕾 Zhang Lei
庄福振 Zhuang Fuzhen		

CN 11-1777 / TP

国内邮发代号:2-654
国外发行代号:M603

定价:78.00元

国内 外 公 开 发 行

万方数据

计算机研究与发展
Jisuanji Yanjiu yu Fazhan
(月刊, 1958年创刊)
第59卷 第10期 2022年10月

主 管	中国科学院
主 办	中国科学院计算技术研究所 中国计算机学会
主 编	徐 志 伟
编辑部主任	侯 丽 珊
编 辑	《计算机研究与发展》编辑部 中国科学院计算技术研究所 地址: 北京中关村科学院南路6号 邮政编码: 100190 电话: +86-10-62620696(兼传真) +86-10-62600350 E-mail: crad@ict.ac.cn https://crad.ict.ac.cn
出 版	科学出版社 地址: 北京东黄城根北街16号 邮政编码: 100717
印刷装订	北京富泰印刷有限责任公司
国内总发行	北京市报刊发行局
订 购 处	全国各邮电局
国外总发行	中国国际图书贸易集团有限公司 北京399信箱 邮政编码: 100044

Journal of Computer
Research and Development
(Monthly, Started in 1958)
Vol.59 No.10 Oct.2022

Supervised by	Chinese Academy of Sciences
Sponsored by	Institute of Computing Technology, Chinese Academy of Sciences China Computer Federation
Editor-in-Chief	Xu Zhiwei
Director	Hou Lishan
Edited by	Editorial Office of <i>Journal of Computer Research and Development</i> Institute of Computing Technology, Chinese Academy of Sciences Add: 6 Kexueyuan South Road, Zhongguancun, Beijing 100190, China Tel: +86-10-62620696 (also Fax) +86-10-62600350 E-mail: crad@ict.ac.cn https://crad.ict.ac.cn
Published by	Science Press Add: 16 Donghuangchenggen North Street, Beijing 100717, China
Printed by	Beijing Futai Printing Co., Ltd.
Distributed by	Beijing Bureau for Distribution of Newspapers and Journals
Domestic	All Local Post Offices in China
Foreign	China International Book Trading Corporation P.O.Box 399, Beijing 100044, China

ISSN 1000-1239



计算机研究与发展

第五十九卷

第十期

二〇二二年十月

科学出版社