

国家发展和改革委员会主管
国家信息中心主办

中文核心期刊
中国科技核心期刊
CSCD来源期刊

信息安全研究

Journal of Information Security Research

第10卷 第1期 2024年1月

Vol.10 No.1 Jan.2024

机密计算发展现状与趋势

安全多方计算应用的隐私度量方法

融合卷积神经网络和Transformer的人脸欺骗检测模型

第1期

CN 10-1345/TP

ISSN 2096-1057



9 772096 105242 01 >

邮发代号：2-41 定价：38.00元

万方数据

信息安全研究

第十卷 第一期

二〇二四年一月

Xinxi Anquan Yanjiu

信息安全研究

(月刊 2015年创刊)

第10卷第1期(总第100期) 2024年1月

主管单位 国家发展和改革委员会

主办单位 国家信息中心

出版单位 《信息安全研究》杂志社有限公司

地址 北京市西城区三里河路58号

邮编 100045

电话 +86(10)68558637

网址 http://www.sicris.cn

电子信箱 ris@cei.cn

执行董事兼社长 李阳

常务副社长 潘静

副主编 马修军 刘蓓

融媒体主编 崔传楨

出版日期 每月5日

国际标准连续出版物号 ISSN 2096-1057

国内统一连续出版物号 CN 10-1345/TP

广告经营许可证 京西市监广登字 20210016号

印刷单位 北京博海升彩色印刷有限公司

国内发行 北京市报刊发行局

订购处 全国各地邮电局(所)

邮发代号 2-41

定价 38.00元

合作单位 360集团 安恒信息

安芯网盾 航天云网

恒安嘉新 绿盟科技

龙象之本 蚂蚁集团

明朝万达 奇安信集团

青藤云安全 深信服科技

数字认证 天融信集团

信安世纪 亚信安全

稿件授权声明: 凡向本刊投稿并被录用, 由本刊支付稿酬的稿件, 均视为稿件作者同意以下条款:

1. 文责自负。 作者保证其拥有该作品的完全著作权(版权), 该作品不涉及政治敏感性和保密问题, 不侵犯任何他人的著作权。

2. 全权许可。 本刊有权以任何形式(包括但不限于通过媒体、网络、光盘等介质)使用、编辑、修改该作品, 无须另行征得作者同意, 无须另行支付稿酬。

3. 独家使用。 未经本刊书面许可, 作者不同意任何单位和个人以任何形式使用(包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版)该作品, 著作权法另有规定的除外。

版权声明: 未经本刊书面许可, 任何单位和个人不得以任何形式使用(包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版)该作品, 著作权法另有规定的除外。

本刊是中文核心期刊(北大核心), 中国科技核心期刊, 中国科学引文数据库(CSCD)来源期刊, 入选CCF T3优秀期刊目录, 全文被《中国核心期刊(遴选)数据库》《中文科技期刊数据库》《CNKI中国期刊全文数据库》《超星期刊域出版平台》《博看网》收录。

» 专家视点

02 机密计算发展现状与趋势..... 冯登国

» 学术论文

06 安全多方计算应用的隐私度量方法
..... 熊维 王海洋 唐祎飞 刘伟

12 基于NTRU密钥协商协议设计
..... 郑鉴学 张道法 徐松艳 宋苏鸣

20 基于国密算法的ModbusTCP协议安全防护与研究
..... 祁志荣 吕世民 郑乾坤

25 融合卷积神经网络和Transformer的人脸欺骗检测模型
..... 黄灵 何希平 贺丹 杨楚天 旷奇弦

34 基于自适应集成学习的异常流量检测
..... 倪嘉翼 陈伟 童家铨 李频

40 基于静态分析和模糊测试的路由器漏洞检测方法
..... 王洪义 沙乐天

48 基于图挖掘的黑灰产运作模式可视分析
..... 尚思佳 陈晓淇 林靖淞 林睫菲 李臻 刘延华

55 金融机构ICT供应链信息安全风险分析及应对措施研究
..... 丁丽媛

61 数字经济伙伴关系协定中个人信息保护研究
..... 张轩诚

67 电力物联网零信任架构下的分布式认证模型
..... 唐大圆 曹翔 林青 胡绍谦 汤震宇

» 技术应用

75 一种虚实结合的工控安全实训靶场平台设计
..... 卢列文 路丹舒 马跃强

81 “RPA+移动存储介质”解决政府数据安全跨网交换的方法与实践
..... 鲁战利 孙贤雯 蔡亮 王佳颖

88 基于零信任安全模型的电力敏感数据访问控制方法
..... 林奕夫 陈雪 许媛媛 汤晓冬 唐仁杰 边珊

94 欧盟网络防御政策研究 赵慧

CONTENTS 目次

Expert Viewpoint

The Status and Trends of Confidential Computing
..... Feng Dengguo (02)

Research Papers

Privacy Measures for Secure Multi-party Computing Applications
..... Xiong Wei, et al (06)

The Design of a Key Agreement Protocol Based on NTRU
..... Zheng Jianxue, et al (12)

Security Protection and Research of ModbusTCP Protocol Based on
National Secret Algorithm Qi Zhirong, et al (20)

Face Spoofing Detection Model with Fusion of Convolutional Neural
Network and Transformer Huang Ling, et al (25)

Abnormal Traffic Detection Based on Adaptive Integrated Learning
..... Ni Jiayi, et al (34)

Router Vulnerability Detection Method Based on Static Analysis and
Fuzzing Wang Hongyi, et al (40)

Visual Analysis of Operation Mode of Black and Grey Production
Based on Graph Mining Shang Sijia, et al (48)

Research on Risk Analysis and Countermeasures of Financial Institution
ICT Supply Chain Information Security Ding Liyuan (55)

Research on the Protection of Personal Information in the Digital
Economy Partnership Agreement Zhang Xuancheng (61)

Distributed Authentication Model Under Power IoT Zero Trust
Architecture Tang Dayuan, et al (67)

Technical Applications

Design of a Virtual and Real Integrated Industrial Control Security
Training Range Platform Lu Liewen, et al (75)

The Method and Practice of “RPA+ Mobile Storage Devices” to Solve
Government Data Cross-network Exchange Safely
..... Lu Zhanli, et al (81)

Power Sensitive Data Access Control Method Based on Zero Trust
Security Model Lin Yifu, et al (88)

Research on the EU Policy on Cyber Defence Zhao Hui (94)

Journal of Information Security Research

Vol.10 No.1 Jan. 2024

Publishing Period: Monthly

Date of Publication: 5th day of each month

International Standard Serial Number:

ISSN 2096-1057

Issues of Domestic Unit: CN 10-1345/TP

Director: Li Yang

Directed by: National Development and Reform
Commission

Sponsored by: The State Information Center

Published by: Journal of Information Security
Research Co., Ltd.

Address: No.58 Sanlihe Road, Xicheng District,
Beijing

Zip Code: 100045

Website: <http://www.sicris.cn>

E-mail: ris@cei.cn

Distributor: Beijing Press and Publication Bureau

Domestic Issue Code: 2-41

Price: 38.00RMB

编委会顾问

蔡吉人 崔书昆 杜虹 方滨兴 冯登国
顾建国 何德全 李京春 吕述望 倪光南
沈昌祥 严明 杨学山 赵战生

编委会主任 王小云

编委会委员

安德智 贝宇红 陈晓桦 陈兴蜀 陈钟
程 度 程学旗 杜彦辉 杜跃进 段海新
范 渊 方 勇 封化民 谷大武 顾 健
郭 莉 郭艳卿 胡爱群 胡红钢 胡红升
黄伟庆 贾 焰 晋 钢 荆继武 姜向前
康海燕 孔祥维 李 晖 李 剑 李建彬
李建华 李守鹏 李 涛 李 小 勇 李欲晓
李舟军 林东岱 林家骏 林雪焰 刘宝旭
刘东红 刘吉强 刘建伟 刘 云 罗森林
马民虎 马 智 孟小峰 潘 泉 彭长根
秦 安 卿 昱 任 奎 任卫红 苏金树
苏 洲 孙德刚 孙 伟 谭晓生 谭毓安
唐春明 滕颖志 田俊峰 田志宏 王宝生
王 标 王 军 王美琴 王志海 王志强
韦 韬 温巧燕 文伟平 韦 韬 翁 健
吴文玲 吴云坤 吴志军 席 卿 肖新光
许光全 许 力 杨 庚 杨满智 杨义先
叶 红 叶晓虎 于 锐 俞能海 云晓春
张 滨 张功萱 张宏莉 张焕国 张 健
张建标 张建军 张庆勇 张仕斌 张小松
张玉清 赵 波 赵淦森 赵有健 郑 东
郑 方 周福才 周琳娜 周 民 周世杰
周 文 朱建明 朱 岩 祝烈煌 邹德清
邹 维

2023山石网科 斩获11项国际荣誉

瞄准世界科技前沿 实现前瞻技术创新

下一代防火墙

- 荣获《2023 Gartner® Peer Insights™ “客户之声” 网络防火墙报告》“客户之选”称号，仅全球两家、国内一家厂商连续四年获此称号
- 被评为沙利文Frost Radar™ “2023年下一代防火墙研究报告” 创新与增长领导者

云工作负载安全

- 山石云铠入选2023年 Gartner® 新兴技术：云工作负载保护平台的采用增长洞察报告
- 山石云铠入选 2023年Gartner® 新兴技术：工作负载运行时可视化领域推荐厂商
- 荣获国际权威网络安全杂志CDM颁发的“下一代云工作负载保护”奖项

网络检测和响应

- 荣获《2023 Gartner® Peer Insights™ “客户之声” NDR报告》“强劲表现者”称号
- 山石智·感入选 2023年 Gartner® 新兴技术：网络检测和响应的采用增长洞察报告
- 山石智·感入选 2023年 Gartner® 新兴技术：网络检测和响应的热门用例
- 被评为沙利文Frost Radar™ “2023年XDR研究报告” 创新与增长领导者

零信任

- 山石网科零信任访问解决方案入选Forrester报告
- 荣获国际权威网络安全杂志CDM颁发的“最佳ZTNA解决方案”奖项



官方微信



官方视频号

弗若斯特沙利文（Frost & Sullivan,简称“沙利文”），全球头部增长咨询公司，1961年成立于华尔街。近年来，沙利文报告被广泛引用于A股、科创板等上市公司的招股文件、一级和二级市场研究报告及其他资本市场公示文件中。

Gartner未在其报告中支持任何厂商、产品或服务，也并不建议技术用户只选择有最高评分或其它特征的厂商。Gartner研究出版物代表的是Gartner研究机构的意见，不应解释为对事实的陈述。

Gartner对与本研究有关的所有明示或暗示的保证概不负责，包括对适用性或特定用途的适用性的任何保证。

Gartner是Gartner 有限公司或其附属公司在美国及全球的注册商标和服务商标，经许可在此使用。保留所有权利。

您优质可靠的伙伴