

主管：中华人民共和国公安部
主办：公安部第三研究所
中国计算机学会



ISSN1671-1122
CN31-1859/TN
中文核心期刊
中国科技核心期刊
中国科学引文数据库来源期刊
CCF计算领域高质量科技期刊

信息网络安全

NETINFO SECURITY

等级保护

量子求解欧拉函数破解RSA算法

技术研究

云边缘环境中基于属性加密的可验证EMR外包解决方案

基于安全两方计算的高效神经网络推理协议

基于云联邦的差分隐私保护动态推荐模型

ISSN 1671-1122



9 771671 112231

2023年 7月 第7期

总第271期



中国计算机学会会刊

☐ 等级保护

- 1 量子求解欧拉函数破解 RSA 算法 张兴兰, 张丰

☐ 技术研究

- 9 云边缘环境中基于属性加密的可验证 EMR 外包解决方案 石润华, 谢晨露
- 22 基于安全两方计算的高效神经网络推理协议 许春根, 薛少康, 徐磊, 张盼
- 31 基于云联邦的差分隐私保护动态推荐模型 刘刚, 杨雯莉, 王同礼, 李阳
- 44 面向区块链金融的抗量子属性基门限环签密方案 俞惠芳, 乔一凡, 孟茹
- 53 基于深度学习的 HTTP 负载隐蔽信道检测方法 苑文昕, 陈兴蜀, 朱毅, 曾雪梅
- 64 基于 AdaN 自适应梯度优化的图像对抗迁移攻击方法 李晨蔚, 张恒巍, 高伟, 杨博
- 74 基于稀疏自动编码器的可解释性异常流量检测 刘宇啸, 陈伟, 张天月, 吴礼发
- 86 基于双通道特征融合的分布式拒绝服务攻击检测算法 蒋英肇, 陈雷, 闫巧

☐ 理论研究

- 98 基于差分隐私和秘密共享的多服务器联邦学习方案 陈晶, 彭长根, 谭伟杰, 许德权

☐ 网域动态

- 111 我国首个区块链技术领域国家标准获批发布
- 112 2023 年《信息安全》西北地区学术研讨会顺利召开
- 113 浙江大学与阿里云合作成果斩获 2023 年 SIGMOD 最佳论文奖
- 114 中国科学家创造城际量子密钥率新纪录

CONTENTS

1	Quantum Solving Euler's Totient Function to Crack RSA.....	ZHANG Xinglan, ZHANG Feng
9	Verifiable Outsourcing EMR Scheme with Attribute-Based Encryption in Cloud-Edge Environments	SHI Runhua, XIE Chenlu
22	Efficient Neural Network Inference Protocol Based on Secure Two-Party Computation.....	XU Chungeng, XUE Shaokang, XU Lei, ZHANG Pan
31	Differential Privacy-Preserving Dynamic Recommendation Model Based on Cloud Federation	LIU Gang, YANG Wenli, WANG Tongli, LI Yang
44	Attribute-Based Anti-Quantum Threshold Ring Signcryption Scheme for Blockchain-Based Finance	YU Huifang, QIAO Yifan, MENG Ru
53	HTTP Payload Covert Channel Detection Method Based on Deep Learning	YUAN Wenxin, CHEN XingShu, ZHU Yi, ZENG XueMei
64	Transferable Image Adversarial Attack Method with AdaN Adaptive Gradient Optimizer	LI Chenwei, ZHANG Hengwei, GAO Wei, YANG Bo
74	Explainable Anomaly Traffic Detection Based on Sparse Autoencoders.....	LIU Yuxiao, CHEN Wei, ZHANG Tianyue, WU Lifa
86	Distributed Denial of Service Attack Detection Algorithm Based on Two-Channel Feature Fusion.....	JIANG Yingzhao, CHEN Lei, YAN Qiao
98	A Multi-Server Federation Learning Scheme Based on Differential Privacy and Secret Sharing	CHEN Jing, PENG Changgen, TAN Weijie, XU Dequan

敬告

本期所有文字和图片未经本刊书面许可,不得转载。

本刊已被中国科技核心期刊、中国科学引文数据库来源期刊、中国学术期刊全文数据库、中文科技期刊数据库(全文版)等数据库收录,如果作者不同意文章被收录,请在来稿时向本刊声明,本刊将做适当处理。