

信息安全学报

Journal of Cyber Security

第 10 卷 第 1 期 2025 年 1 月

目 次

Arm 架构的分支预测器隐蔽信道研究	1
杨 毅, 吴凭飞, 邱朋飞, 王春露, 赵路坦, 张锋巍, 王 博, 吕勇强, 王海霞, 汪东升	
深度学习模型版权保护技术研究综述	17
李珮玄, 黄 土, 罗书卿, 宋佳鑫, 刘功申	
基于身份的联盟链密封电子拍卖协议	36
徐哲清, 王宇航, 王志伟, 刘 峰	
LFDP: 融合低频信息的差分隐私鲁棒性增强方法	47
王 豪, 许 强, 张清华, 李开菊	
面向秘密共享的逐层残差预测加密域大容量数据隐藏	61
温文嫻, 杨育衡, 张玉书, 方玉明, 邱宝林	
物理对抗补丁攻击与防御技术研究综述	75
邓 欢, 黄敏桓, 李 虎, 王 彤, 况晓辉	
基于区块链的大规模线性方程组外包计算方案	91
丁 艳, 王 娜, 杜学绘	
Slice-GCN: 基于程序切片与图神经网络的智能合约漏洞检测方法	105
张人娄, 吴 胜, 张 浩, 刘方宇	
基于生成对抗网络的三维模型识别攻击算法	119
刘 佳, 金志刚, 金诗博	
基于组件分割的钓鱼 URL 检测方法	130
钟文康, 王 添, 张功萱	
基于机器学习的密码算法识别与分析	143
夏锐琪, 李曼曼, 陈少真	
面向云环境的 VMM 平台安全性加固综述	160
周启航, 贾晓启, 张伟娟, 姜 楠	
内部威胁分析与防御综述	176
孙德刚, 刘美辰, 李梅梅, 王 旭, 石志鑫, 刘鹏程, 李 楠	
基于预训练模型的网络空间安全命名实体识别方法	194
韩瑶鹏, 王 璐, 姜 波, 卢志刚, 姜政伟, 刘玉岭	

Journal of Cyber Security

Volume 10 Issue 1 Jan, 2025

Contents

Covert Channel of Branch Predictor on Arm Processor	1
<i>YANG Yi, WU Pingfei, QIU Pengfei, WANG Chunlu, ZHAO Lutan, ZHANG Fengwei, WANG Bo, LYU Yongqiang, WANG Haixia, WANG Dongsheng</i>	
A Survey on Copyright Protection Technology of Deep Learning Model	17
<i>LI Peixuan, HUANG Tu, LUO Shuqing, SONG Jiaxin, LIU Gongshen</i>	
Identity-based Sealed Bid Auction Protocol on Consortium Blockchain	36
<i>XU Zheqing, WANG Yuhang, WANG Zhiwei, LIU Feng</i>	
LFDP: A Differentially Private Robustness Augmentation Method Combining Low-Frequency Information	47
<i>WANG Hao, XU Qiang, ZHANG Qinghua, LI Kaiju</i>	
High-Capacity Data Hiding in Encryption Domain Based on Layer-by-Layer Residual Prediction for Secret Sharing	61
<i>WEN Wenying, YANG Yuheng, ZHANG Yushu, FANG Yuming, QIU Baolin</i>	
A Review on Physical Adversarial Patch Attacks and Defenses Techniques	75
<i>DENG Huan, HUANG Minhuan, LI Hu, WANG Tong, KUANG Xiaohui</i>	
Large-scale Linear Equations Outsourcing Computing Scheme Based on Blockchain	91
<i>DING Yan, WANG Na, DU Xuehui</i>	
Slice-GCN: Smart Contract Vulnerability Detection Based on Program Slicing and Graph Neural Networks	105
<i>ZHANG Renlou, WU Sheng, ZHANG Hao, LIU Fangyu</i>	
The 3D Model Recognition Attack Algorithm based on Generative Adversarial Networks	119
<i>LIU Jia, JIN Zhigang, JIN Shibo</i>	
Phishing URL Detection Method Based on Component Segmentation	130
<i>ZHONG Wenkang, WANG Tian, ZHANG Gongxuan</i>	
Identification and Analysis of Cryptography Algorithms based on Machine Learning	143
<i>XIA Ruiqi, LI Manman, CHEN Shaozhen</i>	
A Survey of VMM Security Reinforcement on Virtualization Platform	160
<i>ZHOU Qihang, JIA Xiaoqi, ZHANG Weijuan, JIANG Nan</i>	
A Survey of Insider Threat Analysis and Defense Solutions	176
<i>SUN Degang, LIU Meichen, LI Meimei, WANG Xu, SHI Zhixin, LIU Pengcheng, LI Nan</i>	
Cybersecurity Named Entity Recognition using the Pre-trained Model	194
<i>HAN Yaopeng, WANG Lu, JIANG Bo, LU Zhigang, JIANG Zhengwei, LIU Yuling</i>	