信息安全学报

Journal of Cyber Security

第 9 卷　　第 5 期　　2024 年 9 月

目　次

大语言模型与网络空间安全

面向威胁情报的大语言模型技术应用综述 ······ *1*
　崔孟娇, 姜政伟, 陈奕任, 江　钧, 张　开, 凌志婷, 封化民, 杨沛安

大语言模型安全的挑战与机遇 ······ *26*
　付志远, 陈思宇, 陈骏帆, 海　翔, 石岩松, 李晓琦, 李益红, 岳秋玲, 张玉清

面向大语言模型的越狱攻击与防御综述 ······ *56*
　梁思源, 何英哲, 刘艾杉, 李京知, 代朋纹, 操晓春

大模型赋能软件供应链开发环节安全研究综述 ······ *87*
　刘井强, 田　星, 舒钰淇, 朱小溪, 刘玉岭, 刘奇旭

基于 **API** 分组重构与图像表示的恶意软件检测分类 ······ *110*
　杨宏宇, 张宇沛, 张　良, 成　翔

保护 **Transformer** 模型知识产权的鲁棒水印 ······ *127*
　王保卫, 郑伟铃

基于图像可视化的恶意软件分类技术综述 ······ *139*
　钱丽萍, 王大伟

基于多视图表示学习的安卓恶意应用检测方法 ······ *162*
　赵文翔, 孟昭逸, 熊　焰, 黄文超

基于无证书的子分组多重签名方案 ······ *178*
　王宇航, 徐哲清, 王志伟, 刘　峰

以太坊非法交易检测方法综述 ······ *189*
　李　梦, 梁广俊, 印　杰, 马　卓, 张　祎

基于改进 **Logistic** 混沌和交叉混沌扩散的强鲁棒性图像加密 ······ *217*
　郭　媛, 贾德宝, 王　充, 翟　平

恶意域名检测方法研究进展 ······ *229*
　王　青, 韩冬旭, 卢志刚, 姜　波, 董　聪, 刘俊荣, 石文昌, 刘玉岭

期刊基本参数：CN 10-1380/TN＊2016＊b＊16＊249＊zh＊P＊ ￥60＊2000＊12＊2024-9

Journal of Cyber Security

Volume 9 Issue 5 Sep, 2024

Contents

Large Language Model and Cyberspace Security

Applications of Large Language Models Technology for Threat Intelligence: A Survey ······ *1*
CUI Mengjiao, JIANG Zhengwei, CHEN Yiren, JIANG Jun, ZHANG Kai, LING Zhiting, FENG Huamin, YANG Peian

Challenges and Opportunities of Large Language Model Security ······ *26*
FU Zhiyuan, CHEN Siyu, CHEN Junfan, HAI Xiang, SHI Yansong, LI Xiaoqi, LI Yihong, YUE Qiuling, ZHANG Yuqing

A Review of Jailbreak Attacks and Defenses for Large Language Models ······ *56*
LIANG Siyuan, HE Yingzhe, LIU Aishan, LI Jingzhi, DAI Pengwen, CAO Xiaochun

A Review of Security Research in the Development Stage of Software Supply Chain Enhanced by Large Models ······ *87*
LIU Jingqiang, TIAN Xing, SHU Yuqi, ZHU Xiaoxi, LIU Yuling, LIU Qixu

Malware Detection and Classification Based on API Block Reconstruction and Image Representation ······ *110*
Yang Hongyu, Zhang Yupei, Zhang Liang, Cheng Xiang

Robust Watermarking for Protect Transformer Intellectual Property ······ *127*
WANG Baowei, ZHENG Weiqian

A Survey on Image Visualization Approaches-based Malware Classification Techniques ······ *139*
QIAN Liping, WANG Dawei

Android Malware Detection Based on Multi-view Representation Learning ······ *162*
ZHAO Wenxiang, MENG Zhaoyi, XIONG Yan, HUANG Wenchao

A Certificateless Subgroup Multi-Signature Scheme ······ *178*
WANG Yuhang, XU Zheqing, WANG Zhiwei, LIU Feng

A Survey of Ethereum Illegal Detection Methods ······ *189*
LI Meng, LIANG Guangjun, YIN Jie, MA Zhuo, ZHANG Yi

Robust Image Encryption Based on Improved Logistic Chaos and Cross-Chaos Diffusion ······ *217*
GUO Yuan, JIA Debao, WANG Chong, ZHAI Ping

Malicious Domain Names Detection Methods Analysis: A Survey ······ *229*
WANG Qing, HAN Dongxu, LU Zhigang, JIANG Bo, DONG Cong, LIU Junrong, SHI Wenchang, LIU Yuling

©Copyright 2023, Institute of Information Engineering, the Chinese Academy of Sciences. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form without the prior written permission of the Institute of Information Engineering, the Chinese Academy of Sciences.