信息安全学报

Journal of Cyber Security

中国计算机学会
CCF

ISSN 2096-1146
05>
9 772096 114206

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

SKLOIS
信息安全国家重点实验室

科学出版社
Science Press

万方数据

目　　次

深度学习模型可解释性的研究进展 ······ *1*

化盈盈, 张岱墀, 葛仕明

人工智能对抗环境下的模型鲁棒性研究综述 ······ *13*

王科迪, 易 平

一种针对多核神经网络处理器的窃取攻击 ······ *23*

高成思, 陈维伟, 王 颖

基于机器学习的僵尸网络 **DGA** 域名检测系统设计与实现 ······ *35*

于光喜, 张 棪, 崔华俊, 杨兴华, 李 杨, 刘 畅

面向无载体信息隐藏的映射关系智能搜索方法 ······ *48*

王亚宁, 吴 槟

基于 **HOG-SVM** 的跳频信号检测识别算法 ······ *62*

张 萌, 王 文, 任俊星, 魏 冬, 黄伟庆, 杨召阳, 吕志强

智能合约安全漏洞研究综述 ······ *78*

倪远东, 张 超, 殷婷婷

DC-Hunter：一种基于字节码匹配的危险智能合约检测方案 ······ *100*

韩松明, 梁 彬, 黄建军, 石文昌

小波域基于差分统计量直方图平移的图像鲁棒可逆信息隐藏算法 ······ *113*

梁幸源, 项世军

期刊基本参数：CN 10-1380/TN＊2016＊b＊16＊127＊zh＊P＊ ￥60＊2000＊9＊2020-05

万方数据

Contents

Research Progress in the Interpretability of Deep Learning Models ······ *1*

HUA Yingying, ZHANG Daichi, GE Shiming

A Survey on Model Robustness under Adversarial Example ······ *13*

WANG Kedi, YI Ping

An Information-leakage Threat Case for Multi-core Neural Network Processor ······ *23*

GAO Chengsi, CHEN Weiwei, WANG Ying

Design and Implementation of A DGA Domain Name Detection System by Machine Learning ······ *35*

YU Guangxi, ZHANG Yan, CUI Huajun, YANG Xinghua, LI Yang, LIU Chang

An intelligent search method of mapping relation for coverless information hiding ······ *48*

WANG Yaning, WU Bin

Detection and Recognition Algorithm for Frequency Hopping Signals Based on HOG-SVM ······ *62*

ZHANG Meng, WANG Wen, REN Junxing, WEI Dong, HUANG Weiqing, YANG Zhaoyang, LV Zhiqiang

A Survey of Smart Contract Vulnerability Research ······ *78*

NI Yuandong, ZHANG Chao, YIN Tingting

DC-Hunter：Detecting Dangerous Smart Contracts via Bytecode Matching ······ *100*

HAN Songming, LIANG Bin, HUANG Jianjun, SHI Wenchang

Robust and Reversible Data Hiding Algorithm Based on Histogram of Difference Statistics Shifting in Wavelet Domain ······ *113*

LIANG Xingyuan, XIANG Shijun

©Copyright 2016, 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.

万方数据