2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2020)

Guangzhou, China
29 December 2020 - 1 January 2021

Pages 1-682

IEEE Catalog Number: CFP20TRU-POD
ISBN: 978-1-6654-0393-1

Copyright © 2020 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP20TRU-POD
ISBN (Print-On-Demand):	978-1-6654-0393-1
ISBN (Online):	978-1-6654-0392-4
ISSN:	2324-898X

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)

TrustCom 2020

Table of Contents

Welcome Messages from IEEE TrustCom 2020 General Chairs xliii
Welcome Messages from IEEE TrustCom 2020 Program Chairs xliv
IEEE TrustCom 2020 Organizing and Program Committees xlv
C4W 2020 Organizing and Program Committees lv
AEIT 2020 Organizing and Program Committees lviii
PASS4IoT 2020 Organizing and Program Committees lx
IWCSS 2020 Organizing and Program Committees lxi
BlockchainSys 2020 Organizing and Program Committees lxiv
MLTrustCom 2020 Organizing and Program Committees lxvi
SmartITC 2020 Organizing and Program Committees lxvii

The 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020)

Session TrustCom-1

TT - Trust Track

Enhancing Randomization Entropy of x86-64 Code while Preserving Semantic Consistency 1
Xuewei Feng (National Key Laboratory of Science and Technology on Information System Security, China), Dongxia Wang (National Key Laboratory of Science and Technology on Information System Security, China), Zhechao Lin (National Key Laboratory of Science and Technology on Information System Security, China), Xiaohui Kuang (National Key Laboratory of Science and Technology on Information System Security, China), and Gang Zhao (National Key Laboratory of Science and Technology on Information System Security, China)

Reversible Data Hiding Based on Improved Rhombus Predictor and Prediction Error Expansion 13
Xin Tang (University of International Relations, China), Linna Zhou (Beijing University of Posts and Telecommunications, China), Dan Liu (University of International Relations, China), Boyu Liu (University of International Relations, China), and Xinyi Lü (University of International Relations, China)

A Trust Routing Scheme Based on Identification of Non-complete Cooperative Nodes in Mobile Peer-to-Peer Networks 22
Dapeng Qu (Liaoning University, China), Jiankun Zhang (Liaoning University, China), Zhenhuan Hou (Liaoning University, China), Min Wang (Liaoning University, China), and Bo Dong (Liaoning University, China)

SeRoT: A Secure Runtime System on Trusted Execution Environments 30
Jingbin Liu (TCA&SKLCS, Institute of Software, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yu Qin (TCA&SKLCS, Institute of Software, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Dengguo Feng (TCA&SKLCS, Institute of Software, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

Robust Scheduling for Large-Scale Distributed Systems 38
Young Choon Lee (Macquarie University, Australia), Jayden King (Macquarie University, Australia), Young Ki Kim (The University of Sydney, Australia), and Seok-Hee Hong (The University of Sydney, Australia)

Adaptive Random Test Case Generation Based on Multi-objective Evolutionary Search 46
Chengying Mao (Jiangxi University of Finance and Economics, China), Linlin Wen (Jiangxi University of Finance and Economics, China), and Tsong Yueh Chen (Swinburne University of Technology, Australia)

Improving Efficiency of Key Enumeration Based on Side-Channel Analysis 54
Wei Yang (Nanjing University of Science and Technology, China), Anmin Fu (Nanjing University of Science & Technology, China), Hailong Zhang (State Key Laboratory of Cryptology, China), and Chanying Huang (Nanjing University of Science & Technology, China)

Robust Spatial-Spread Deep Neural Image Watermarking 62
Marcin Plata (Wrocław University of Science and Technology, Poland; Vestigit, Wrocław, Poland) and Piotr Syga (Wrocław University of Science and Technology, Poland; Vestigit, Wrocław, Poland)

DeM-CoD: Novel Access-Control-Based Cash on Delivery Mechanism for Decentralized Marketplace 71
Xuan Son Ha (FPT University, Vietnam), Hai Trieu Le (Can Tho University of Technology, Vietnam), Nadia Metoui (University of Amsterdam, Netherlands), and Nghia Duong-Trung (FPT University, Vietnam)

Modeling and Analysis of RabbitMQ Using UPPAAL 79
Ran Li (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Jiaqi Yin (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), and Huibiao Zhu (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China)

User-Controlled, Auditable, Cross-Jurisdiction Sharing of Healthcare Data Mediated by a Public Blockchain 87
Xiaohu Zhou (Birmingham City University, UK), Vitor Jesus (Birmingham City University, UK), Yonghao Wang (Birmingham City University, UK), and Mark Josephs (Birmingham City University, UK)

A Unified Host-Based Intrusion Detection Framework using Spark in Cloud .97
Ming Liu (Shanghai Jiao Tong University, China), Zhi Xue (Shanghai Jiao Tong University, China), and Xiangjian (Sean) He (University of Technology Sydney, Australia)

TA-HRT: A Temperature-Aware Scheduler for Heterogeneous Real-Time Multicore Systems .104
Yanshul Sharma (IIIT Guwahati, India), Zinea Das (IIIT Guwahati, India), Alok Das (IIIT Guwahati, India), and Sanjay Moulik (IIIT Guwahati, India)

Reducing the Price of Protection: Identifying and Migrating Non-sensitive Code in TEE .112
Yin Liu (Software Innovations Lab, Virginia Tech) and Eli Tilevich (Software Innovations Lab, Virginia Tech)

Fairness Testing of Machine Learning Models Using Deep Reinforcement Learning .121
Wentao Xie (University of Chinese Academy of Sciences, China) and Peng Wu (University of Chinese Academy of Sciences, China)

ST - Security Track

Cyclic Bayesian Attack Graphs: A Systematic Computational Approach .129
Isaac Matthews (Newcastle University, U.K.), John Mace (Newcastle University, U.K.), Sadegh Soudjani (Newcastle University, U.K.), and Aad van Moorsel (Newcastle University, U.K.)

Practical Secure Two-Party EdDSA Signature Generation with Key Protection and Applications in Cryptocurrency .137
Qi Feng (Key Laboratory of Aerospace Information Security and Trusted Computing, Wuhan University, China), Debiao He (Key Laboratory of Aerospace Information Security and Trusted Computing, Wuhan University, China), Min Luo (Key Laboratory of Aerospace Information Security and Trusted Computing, Wuhan University, China), Zengxiang Li (Digital Research Institute, ENN Group, China), and Kim-Kwang Raymond Choo (University of Texas at San Antonio, China)

Password Policies vs. Usability: When Do Users Go "Bananas"? .148
Roberto Dillon (James Cook University Singapore), Shailey Chawla (James Cook University Singapore), Dayana Hristova (Cognitive Science Hub, University of Vienna, Austria), Barbara Göbl (Research Group Entertainment Computing, University of Vienna, Austria), and Suzana Jovicic (University of Vienna, Austria)

Malware Classification on Imbalanced Data through Self-Attention .154
Yu Ding (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), ShuPeng Wang (Institute of Information Engineering, Chinese Academy of Sciences, China), Jian Xing (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China; National Computer Network Emergency Response Technical Team/Coordination Center of China Xinjiang Branch, China), XiaoYu Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China), ZiSen Qi (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China), Ge Fu (National Computer Network Emergency Response Technical Team/Coordination Center of China, China), Qian Qiang (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences, China; National Computer Network Emergency Response Technical Team/Coordination Center of China, China), HaoLiang Sun (National Computer Network Emergency Response Technical Team/Coordination Center of China, China), and JianYu Zhang (Changan Communication Technology Co., LTD., China)

Novel Design of Hardware Trojan: A Generic Approach for Defeating Testability Based Detection .162
Ning Zhang (Institute of Information Engineering, CAS, China; University of Chinese Academy of Sciences, China), Zhiqiang Lv (Institute of Information Engineering, Chinese Academy of Sciences, China), Yanlin Zhang (University of Chinese Academy of Sciences, China), Haiyang Li (University of Chinese Academy of Sciences, China), Yixin Zhang (University of Chinese Academy of Sciences, China), and Weiqing Huang (Institute of Information Engineering, Chinese Academy of Sciences, China)

TRUVIN: Lightweight Detection of Data Oriented Attacks Through Trusted Value Integrity .174
Munir Geden (University of Oxford, United Kingdom) and Kasper Rasmussen (University of Oxford, United Kingdom)

LURK: Server-Controlled TLS Delegation .182
Ioana Boureanu (University of Surrey), Daniel Migault (Ericsson Security), Stere Preda (Ericsson Security), Hyame Assem Alamedine (Ericsson Security), Sanjay Mishra (Verizon), Frederic Fieau (Orange), and Mohammad Mannan (Concordia University)

Malware Detection Based on Term Frequency Analysis of GPRs Features .194
Fang Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ziyuan Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Chao Yan (Institute of Information Engineering, Chinese Academy of Sciences, China), Bowen Chen (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Dan Meng (Institute of Information Engineering, Chinese Academy of Sciences, China)

Secure Outsourcing of Multi-armed Bandits 202
Radu Ciucanu (INSA Centre Val de Loire, LIFO), Pascal Lafourcade (Univ. Clermont Auvergne, LIMOS), Marius Lombard-Platet (Univ. PSL, DIENS, Be-Studys), and Marta Soare (Univ. Orléans, LIFO)

NLabel: An Accurate Familial Clustering Framework for Large-Scale Weakly-Labeled Malware 210
Yannan Liu (Sangfor Technologies Inc.; Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China), Yabin Lai (Sangfor Technologies Inc.), Kaizhi Wei (Sangfor Technologies Inc.), Liang Gu (Sangfor Technologies Inc.), and Zhengzheng Yan (Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China)

Active Link Obfuscation to Thwart Link-Flooding Attacks for Internet of Things 217
Xuyang Ding (University of Electronic Science and Technology of China, China), Feng Xiao (Wuhan University, China), Man Zhou (Wuhan University, China), and Zhibo Wang (Wuhan University, China)

VALID: Voltage-Based Lightweight Intrusion Detection for the Controller Area Network 225
Oleg Schell (Bosch Engineering GmbH, Germany) and Marcel Kneib (Robert Bosch GmbH, Germany)

Densely Connected Residual Network for Attack Recognition 233
Peilun Wu (University of New South Wales, Sydney; Sangfor Technologies Inc.), Nour Moustafa (Australian Center for Cyber, University of New South Wales, Canberra), Shiyi Yang (University of New South Wales, Sydney), and Hui Guo (University of New South Wales, Sydney)

Optimized FPGA Implementation of Elliptic Curve Cryptosystem over Prime Fields 243
Guoqiang Yang (Shandong University, China), Fanyu Kong (Shandong University, China), and Qiuliang Xu (Shandong University, China)

FTPB: A Three-Stage DNS Tunnel Detection Method Based on Character Feature Extraction 250
Kemeng Wu (Institute of Information Engineering, Chinese Academy of Sciences, University of Chinese Academy of Sciences, China), Yongzheng Zhang (Institute of Information Engineering, Chinese Academy of Sciences, University of Chinese Academy of Sciences, China), and Tao Yin (Institute of Information Engineering, Chinese Academy of Sciences, University of Chinese Academy of Sciences, China)

De-Randomizing the Code Segment with Timing Function Attack 259
Tianning Zhang (Nanjing University, China), Miao Cai (Nanjing University, China), Diming Zhang (Jiangsu University of Science and Technology, China), and Hao Huang (Nanjing University, China)

Unmasking Windows Advanced Persistent Threat Execution 268
Rory Coulter (Swinburne University of Technology, Australia), Jun Zhang (Swinburne University of Technology, Australia), Lei Pan (Deakin University, Australia), and Yang Xiang (Swinburne University of Technology, Australia)

Ciphertext-Policy Attribute-Based Encryption with Multi-keyword Search over Medical Cloud Data 277
Changchun Yin (Nanjing University of Aeronautics and Astronautics, China), Hao Wang (Nanjing University of Aeronautics and Astronautics, China), Lu Zhou (Nanjing University of Aeronautics and Astronautics, China), and Liming Fang (Nanjing University of Aeronautics and Astronautics, China)

VCKSCF: Efficient Verifiable Conjunctive Keyword Search Based on Cuckoo Filter for Cloud Storage .285
Chan Fan (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Xiaolei Dong (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Zhenfu Cao (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China; Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen and Shanghai Institute of Intelligent Science and Technology, Tongji University, China), and Jiachen Shen (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China)

Program Slice Based Vulnerable Code Clone Detection .293
Xiaonan Song (Institute of Information Engineering, Chinese Academy of Sciences, China), Aimin Yu (Institute of Information Engineering, Chinese Academy of Sciences, China), Haibo Yu (Institute of Information Engineering, Chinese Academy of Sciences, China), Shirun Liu (Institute of Information Engineering, Chinese Academy of Sciences, China), Xin Bai (Institute of Information Engineering, Chinese Academy of Sciences, China), Lijun Cai (Institute of Information Engineering, Chinese Academy of Sciences, China), and Dan Meng (Institute of Information Engineering, Chinese Academy of Sciences, China)

Doc2vec-Based Insider Threat Detection through Behaviour Analysis of Multi-source Security Logs .301
Liu Liu (Swinburne University of Technology, Australia), Chao Chen (James Cook University, Australia), Jun Zhang (Swinburne University of Technology, Australia), Olivier De Vel (Defence Science and Technology Group, Australia), and Yang Xiang (Swinburne University of Technology, Australia)

C2BID: Cluster Change-Based Intrusion Detection .310
Tiago Fernandes (CINAMIL, Academia Militar, Instituto Universitário Militar – Portugal; INESC-ID, Instituto Superior Técnico, Universidade de Lisboa – Portugal), Luis Dias (CINAMIL, Academia Militar, Instituto Universitário Militar – Portugal; INESC-ID, Instituto Superior Técnico, Universidade de Lisboa – Portugal), and Miguel Correia (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa – Portugal)

TEADS: A Defense-Aware Framework for Synthesizing Transient Execution Attacks .320
Tianlin Huo (University of Chinese Academy of Sciences; Institute of Software, Chinese Academy of Sciences), Wenhao Wang (Institute of Information Engineering, Chinese Academy of Sciences), Pei Zhao (Institute of Software, Chinese Academy of Sciences), Yufeng Li (University of Chinese Academy of Sciences; Institute of Software, Chinese Academy of Sciences), Tingting Wang (University of Chinese Academy of Sciences; Institute of Information Engineering, Chinese Academy of Sciences), and Mingshu Li (Institute of Software, Chinese Academy of Sciences)

One Covert Channel to Rule Them All: A Practical Approach to Data Exfiltration in the Cloud .328
Benjamin Semal (Information Security Group, Royal Holloway University of London, United Kingdom), Konstantinos Markantonakis (Information Security Group, Royal Holloway University of London, United Kingdom), Keith Mayes (Information Security Group, Royal Holloway University of London, United Kingdom), and Jan Kalbantner (Information Security Group, Royal Holloway University of London, United Kingdom)

ReDex: Unpacking Android Packed Apps by Executing Every Method .337
Jiajin Cai (Peking University, China), Tongxin Li (Peking University, China), Can Huang (Peking University, China), and Xinhui Han (Peking University, China)

Awareness of Secure Coding Guidelines in the Industry - A First Data Analysis .345
Tiago Espinha Gasiba (Siemens AG, Germany), Ulrike Lechner (Universität der Bundeswehr München, Germany), Maria Pinto-Albuquerque (Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-IUL, Lisboa, Portugal), and Daniel Mendez Fernandez (Blekinge Institute of Technology, Karlskrona, Sweden)

IoT Attacks: Features Identification and Clustering .353
Junaid Haseeb (Victoria University of Wellington, New Zealand), Masood Mansoori (Victoria University of Wellington, New Zealand), Harith Al-Sahaf (Victoria University of Wellington, New Zealand), and Ian Welch (Victoria University of Wellington, New Zealand)

Estimating Loss Due to Cyber-Attack in the Presence of Uncertainty .361
Hoang Hai Nguyen (Information Trust Institute, University of Illinois at Urbana-Champaign) and David M. Nicol (Information Trust Institute, University of Illinois at Urbana-Champaign)

STIDM: A Spatial and Temporal Aware Intrusion Detection Model .370
Xueying Han (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Rongchao Yin (China Academy of Industrial Internet, China), Zhigang Lu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Bo Jiang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yuling Liu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Song Liu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Chonghua Wang (China Industrial Control Systems Cyber Emergency Response Team, China), and Ning Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

Partial-SMT: Core-Scheduling Protection Against SMT Contention-Based Attacks .378
Xiaohui Wu (Institute of Software Chinese Academy of Sciences, China), Yeping He (Institute of Software Chinese Academy of Sciences, China), Qiming Zhou (Institute of Software Chinese Academy of Sciences, China), Hengtai Ma (Institute of Software Chinese Academy of Sciences, China), Liang He (Institute of Software Chinese Academy of Sciences, China), Wenhao Wang (Institute of Information Engineering Chinese Academy of Sciences, China), and Liheng Chen (Institute of Software Chinese Academy of Sciences, China)

Family Identification of AGE-Generated Android Malware Using Tree-Based Feature .386
Guga Suri (Wuhan University, China), Jianming Fu (Wuhan University, China), Rui Zheng (Wuhan University, China), and Xinying Liu (China Merchants Financia, China)

Towards a Theory of Special-Purpose Program Obfuscation .394
Muhammad Rizwan Asghar (The University of Auckland, New Zealand), Steven Galbraith (The University of Auckland, New Zealand), Andrea Lanzi (Universita degli studi di Milano, Italy), Giovanni Russello (The University of Auckland, New Zealand), and Lukas Zobernig (The University of Auckland, New Zealand)

Protecting the Intellectual Property of Deep Neural Networks with Watermarking: The Frequency Domain Approach .402
Meng Li (Wuhan University of Technology, Wuhan, China), Qi Zhong (Deakin University, Geelong, Australia), Leo Yu Zhang (Deakin University, Geelong, Australia), Yajuan Du (Wuhan University of Technology, Wuhan, China), Jun Zhang (Swinburne University of Technology, Melbourne, Australia), and Yong Xiang (Deakin University, Geelong, Australia)

Uncovering the Hidden Dangers: Finding Unsafe Go Code in the Wild .410
Johannes Lauinger (Technische Universität Darmstadt, Germany), Lars Baumgärtner (Technische Universität Darmstadt, Germany), Anna-Katharina Wickert (Technische Universität Darmstadt, Germany), and Mira Mezini (Technische Universität Darmstadt, Germany)

Traffic Classification of User Behaviors in Tor, I2P, ZeroNet, Freenet .418
Yuzong Hu (Shanghai Jiao Tong University, China), Futai Zou (Shanghai Jiao Tong University, China), Linsen Li (Shanghai Jiao Tong University, China), and Ping Yi (Shanghai Jiao Tong University, China)

MAUSPAD: Mouse-Based Authentication Using Segmentation-Based, Progress-Adjusted DTW .425
Dong Qin (Iowa State University, USA), Shen Fu (Iowa State University, USA), George Amariucai (Kansas State University, USA), Daji Qiao (Iowa State University, USA), and Yong Guan (Iowa State University, USA)

Improving the Effectiveness of Grey-box Fuzzing by Extracting Program Information .434
Yu Fu (University of Chinese Academy of Sciences; TCA Lab, Institute of Software Chinese Academy of Sciences), Siming Tong (University of Chinese Academy of Sciences; TCA Lab, Institute of Software Chinese Academy of Sciences), Xiangyu Guo (Beijing University of Posts and Telecommunications), Liang Cheng (TCA Lab, Institute of Software Chinese Academy of Sciences), Yang Zhang (TCA Lab, Institute of Software Chinese Academy of Sciences), and Dengguo Feng (TCA Lab, Institute of Software Chinese Academy of Sciences)

Evaluating the Soundness of Security Metrics from Vulnerability Scoring Frameworks ..442
Joe Samuel (Systems and Computer Engineering, Carleton University, Canada), Khalil Aalab (Systems and Computer Engineering, Carleton University, Canada), and Jason Jaskolka (Systems and Computer Engineering, Carleton University, Canada)

SpeedNeuzz: Speed Up Neural Program Approximation with Neighbor Edge Knowledge ..450
Yi Li (Tsinghua university, China; Cyberspace Security Research Center, Peng Cheng Laboratory, China), Xi Xiao (Cyberspace Security Research Center, Peng Cheng Laboratory, China), Xiaogang Zhu (Cyberspace Security Research Center, Peng Cheng Laboratory, China), Xiao Chen (Faculty of Information Technology, Monash University, Melbourne, Australia), Sheng Wen (Tsinghua university, China; Cyberspace Security Research Center, Peng Cheng Laboratory, China), and Bin Zhang (Tsinghua university, China; Cyberspace Security Research Center, Peng Cheng Laboratory, China)

Mind the GAP: Security & Privacy Risks of Contact Tracing Apps ..458
Lars Baumgärtner (Technische Universität Darmstadt, Germany), Alexandra Dmitrienko (Julius-Maximilians-Universität Würzburg, Germany), Bernd Freisleben (Philipps-Universität Marburg, Germany), Alexander Gruler (Technische Universität Darmstadt, Germany), Jonas Höchst (Technische Universität Darmstadt, Germany; Philipps-Universität Marburg, Germany), Joshua Kühlberg (Technische Universität Darmstadt, Germany), Mira Mezini (Technische Universität Darmstadt, Germany), Richard Mitev (Technische Universität Darmstadt, Germany), Markus Miettinen (Technische Universität Darmstadt, Germany), Anel Muhamedagic (Technische Universität Darmstadt, Germany), Thien Duc Nguyen (Technische Universität Darmstadt, Germany), Alvar Penning (Philipps-Universität Marburg, Germany), Dermot Pustelnik (Technische Universität Darmstadt, Germany), Filipp Roos (Julius-Maximilians-Universität Würzburg, Germany), Ahmad-Reza Sadeghi (Technische Universität Darmstadt, Germany), Michael Schwarz (Philipps-Universität Marburg, Germany), and Christian Uhl (Philipps-Universität Marburg, Germany)

Far from Classification Algorithm: Dive into the Preprocessing Stage in DGA Detection ..468
Mingkai Tong (NSFOCUS Technologies Group Co., Ltd., China), Guo Li (Tsinghua University, China), Runzi Zhang (NSFOCUS Technologies Group Co., Ltd., China; Tsinghua University, China), Jianxin Xue (NSFOCUS Technologies Group Co., Ltd., China; Tsinghua University, China), Wenmao Liu (NSFOCUS Technologies Group Co., Ltd., China), and Jiahai Yang (Tsinghua University, China)

ELPPS: An Enhanced Location Privacy Preserving Scheme in Mobile Crowd-Sensing Network Based on Edge Computing ..475
Minghui Li (Nanjing University of Aeronautics and Astronautics, China), Yang Li (Nanjing University of Aeronautics and Astronautics, China), and Liming Fang (Nanjing University of Aeronautics and Astronautics, China)

Phishing Web Page Detection Using Optimised Machine Learning ..483
Jordan Stobbs (Northumbria University, UK), Biju Issac (Northumbria University, UK), and Seibu Mary Jacob (Teesside University, UK)

Asset-Oriented Threat Modeling .491
Nan Messe (IRISA, France), Vanea Chiprianov (DiverSE, IRISA, France), Nicolas Belloir (DiverSE, IRISA, France), Jamal El-Hachem (DiverSE, IRISA, France), Régis Fleurquin (DiverSE, IRISA, France), and Salah Sadou (DiverSE, IRISA, France)

All Your PLCs Belong to Me: ICS Ransomware Is Realistic .502
Yipeng Zhang (Beihang University, China), Zhonghao Sun (CNCERT/CC, China), Liqun Yang (Beihang University, China), Zhoujun Li (Beihang University, China), Qiang Zeng (University of South Carolina, China), Yueying He (CNCERT/CC, China), and Xiaoming Zhang (CNCERT/CC, China)

Automated Enforcement of the Principle of Least Privilege over Data Source Access .510
Haoqi Wu (Laboratory for Data Analytics and Security, Fudan University, China), Zhengxuan Yu (Laboratory for Data Analytics and Security, Fudan University, China), Dapeng Huang (Laboratory for Data Analytics and Security, Fudan University, China), Haodong Zhang (Laboratory for Data Analytics and Security, Fudan University, China), and Weili Han (Laboratory for Data Analytics and Security, Fudan University, China)

Extending Registration and Authentication Processes of FIDO2 External Authenticator with QR Codes .518
Chengqian Guo (Institute of Information Engineering, Chinese Academy of Sciences, China; Data Assurance and Communication Security Research Center, CAS; University of Chinese Academy of Sciences), Quanwei Cai (Institute of Information Engineering, Chinese Academy of Sciences, China; Data Assurance and Communication Security Research Center, CAS; University of Chinese Academy of Sciences), Qiongxiao Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; Data Assurance and Communication Security Research Center, CAS; University of Chinese Academy of Sciences), and Jingqiang Lin (University of Science and Technology of China, China)

BHDA - A Blockchain-Based Hierarchical Data Access Model for Financial Services .530
Zhiyu Xu (Swinburne University of Technology, Australia), Lin Yang (Swinburne University of Technology, Australia), Ziyuan Wang (Swinburne University of Technology, Australia), Sheng Wen (Pengcheng Lab, China), Rob Hanson (The Commonwealth Scientific and Industrial Research Organisation, Australia), Shiping Chen (The Commonwealth Scientific and Industrial Research Organisation, Australia), and Yang Xiang (Swinburne University of Technology, Australia)

FTCLNet: Convolutional LSTM with Fourier Transform for Vulnerability Detection .539
Defu Cao (Peking University, China), Jing Huang (Peking University, China), Xuanyu Zhang (Beijing Normal University, China), and Xianhua Liu (Peking University, China)

Secure Coded Matrix Multiplication Against Cooperative Attack in Edge Computing .547
Luqi Zhu (Computer Science and Technology, Soochow University, China), Jin Wang (Computer Science and Technology, Soochow University, China), Lianmin Shi (Computer Science and Technology, Soochow University, China), Jingya Zhou (Computer Science and Technology, Soochow University, China), Kejie Lu (Computer Science and Engineering, University of Puerto Rico at Mayagüez, Puerto Rico), and Jianping Wang (Computer Science, City University of Hong Kong, China)

A Measurement Study of IoT-Based Attacks Using IoT Kill Chain .557
Junaid Haseeb (Victoria University of Wellington, New Zealand), Masood Mansoori (Victoria University of Wellington, New Zealand), and Ian Welch (Victoria University of Wellington, New Zealand)

Modeling and Verification of Spatio-Temporal Intelligent Transportation Systems .568
Tengfei Li (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Xiaohong Chen (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Haiying Sun (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Jing Liu (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Jiajia Yang (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Chenchen Yang (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), and Junfeng Sun (Casco Signal Ctd., China)

Secure Outsourcing Algorithms of Modular Exponentiations in Edge Computing .576
Tianyi Zhang (Nanjing University of Aeronautics and Astronautics) and Jian Wang (Nanjing University of Aeronautics and Astronautics)

Joint Learning for Document-Level Threat Intelligence Relation Extraction and Coreference Resolution Based on GCN .584
Xuren Wang (Capital Normal University, China), Mengbo Xiong (Capital Normal University, China), Yali Luo (Institute of Information Engineering, Chinese Academy of Sciences, University of Chinese Academy of Sciences, China), Ning Li (Institute of Information Engineering, Chinese Academy of Sciences, University of Chinese Academy of Sciences, China), Zhengwei Jiang (Institute of Information Engineering, Chinese Academy of Sciences, University of Chinese Academy of Sciences, China), and Zihan Xiong (Capital Normal University, China)

Anomaly Detection on MIL-STD-1553 Dataset using Machine Learning Algorithms .592
Francis Onodueze (Bowie State University, USA) and Darsana Josyula (Bowie State University, USA)

PT - Privacy Track

Privacy-Preserving Ride-Hailing with Verifiable Order-Linking in Vehicular Networks .599
Meng Li (Hefei University of Technology, China), Jianbo Gao (Hefei University of Technology, China), Yifei Chen (Hefei University of Technology, China), Jingcheng Zhao (Hefei University of Technology, China), and Mamoun Alazab (Charles Darwin University, Australia)

Flowverine: Leveraging Dataflow Programming for Building Privacy-Sensitive Android Applications .607
Eduardo Gomes (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa, Portugal), Igor Zavalyshyn (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa, Portugal; UCLouvain, ICTEAM, Louvain-la-Neuve, Belgium), Nuno Santos (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa, Portugal), João Silva (INESC-ID / Instituto Superior Técnico, Universidade de Lisboa, Portugal), and Axel Legay (UCLouvain, ICTEAM, Louvain-la-Neuve, Belgium)

Prihook: Differentiated Context-Aware Hook Placement for Different Owners' Smartphones .615..
Chen Tian (Institute of Information Engineering, Chinese Academy of Sciences), Yazhe Wang (Institute of Information Engineering, Chinese Academy of Sciences), Peng Liu (Pennsylvania State University), Yu Wang (Institute of Information Engineering, Chinese Academy of Sciences), Ruirui Dai (Institute of Information Engineering, Chinese Academy of Sciences), Anyuan Zhou (Institute of Information Engineering, Chinese Academy of Sciences), and Zhen Xu (Institute of Information Engineering, Chinese Academy of Sciences)

Improving Laplace Mechanism of Differential Privacy by Personalized Sampling .623.....
Wen Huang (University of Electronic Science and Technology of China, China), Shijie Zhou (University of Electronic Science and Technology of China, China), Tianqing Zhu (University of Technology Sydney, China), Yongjian Liao (University of Electronic Science and Technology of China, China), Chunjiang Wu (University of Electronic Science and Technology of China, China), and Shilin Qiu (University of Electronic Science and Technology of China, China)

Differential Privacy Preservation in Interpretable Feedforward-Designed Convolutional Neural Networks .631.....
De Li (Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, China), Jinyan Wang (Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, China), Zhou Tan (Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, China), Xianxian Li (Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, China), and Yuhang Hu (Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, China)

Practical and Secure Circular Range Search on Private Spatial Data .639.....
Zhihao Zheng (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Zhenfu Cao (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China; Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen and Shanghai Institute of Intelligent Science and Technology, Tongji University, China), and Jiachen Shen (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China)

Dataset Construction and Analysis of Screenshot Malware .646.....
Hugo Sbaï (University of Oxford, UK), Jassim Happa (Royal Holloway, University of London, UK), Michael Goldsmith (University of Oxford, UK), and Samy Meftali (Université de Lille 1, France)

zkrpChain: Privacy-Preserving Data Auditing for Consortium Blockchains Based on Zero-Knowledge Range Proofs .656.....
Shiwei Xu (Huazhong Agricultural University, China), Xiaowen Cai (Huazhong Agricultural University, China), Yizhi Zhao (Huazhong Agricultural University, China), Zhengwei Ren (Wuhan University of Science and Technology, China), Lingjuan Wu (Huazhong Agricultural University, China), Huanguo Zhang (Wuhan University, China), Le Du (Wuhan Donghu Big Data Trading Center Co. Ltd., China), and Yan Tong (Huazhong Agricultural University, China)

On the Role of Data Anonymization in Machine Learning Privacy .664
Navoda Senavirathne (University of Skövde, Sweden) and Vicenç Torra (University of Umeå, Sweden)

Heimdall: Illuminating the Hidden Depths of Third-Party Tracking in Android Applications .676
Thomas Cory (Technische Universität Berlin, Germany), Philip Raschke (Technische Universität Berlin, Germany), and Axel Küpper (Technische Universität Berlin, Germany)

A Privacy-Preserving Data Collection and Processing Framework for Third-Party UAV Services .683
Tianyuan Liu (University of Illinois at Urbana-Champaign), Hongpeng Guo (University of Illinois at Urbana-Champaign), Claudiu Danilov (Boeing Research & Technology), and Klara Nahrstedt (University of Illinois at Urbana-Champaign)

On the Comparison of Classifiers' Construction over Private Inputs .691
Mina Sheikhalishahi (Eindhoven University of Technology, Netherlands) and Nicola Zannone (Eindhoven University of Technology, Netherlands)

Napping Guard: Deanonymizing Tor Hidden Service in a Stealthy Way .699
Muqian Chen (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Xuebin Wang (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Jinqiao Shi (Beijing University of Posts and Telecommunications; Institute of Information Engineering, Chinese Academy of Sciences), Can Zhao (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Meiqi Wang (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences), and Binxing Fang (Institute of Information Engineering, Chinese Academy of Sciences; Electronic and Information Engineering of UESTC in Guangdong)

Multi-party Private Set Intersection in Vertical Federated Learning .707
Linpeng Lu (Shanghai JiaoTong University, China) and Ning Ding (Shanghai Jiao Tong University, China)

F&AT - Forensics and Analytics Track

MLTracer: Malicious Logins Detection System via Graph Neural Network .715
Fucheng Liu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yu Wen (Institute of Information Engineering, Chinese Academy of Sciences, China), Yanna Wu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Shuangshuang Liang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xihe Jiang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Dan Meng (Institute of Information Engineering, Chinese Academy of Sciences, China)

Data Analytics-Enabled Intrusion Detection: Evaluations of ToN_IoT Linux Datasets .727
Nour Moustafa (University of New South Wales, Canberra, Australia), Mohiuddin Ahmedy (Edith Cowan University, Perth, Australia), and Sherif Ahmed (University of Windsor, Windsor, Canada)

CMIRGen: Automatic Signature Generation Algorithm for Malicious Network Traffic .736
Runzi Zhang (NSFOCUS Technologies Group Co., Ltd., China; Tsinghua University, China), MingKai Tong (NSFOCUS Technologies Group Co., Ltd., China), Lei Chen (NSFOCUS Technologies Group Co., Ltd., China; Tsinghua University, China), Jianxin Xue (NSFOCUS Technologies Group Co., Ltd., China; Tsinghua University, China), Wenmao Liu (NSFOCUS Technologies Group Co., Ltd., China), and Feng Xie (Harbin Engineering University, China)

A Novel Violation Tracing Model for Cloud Service Accountability .744
Xiaojian Li (Guangxi Normal University, China), Bo Li (Guangxi Normal University, China), Hailan Wang (Guangxi Normal University, China), Jiajia Zhang (Guangxi Normal University, China), Haopeng Yang (Guangxi Normal University, China), and Jingang Liu (Beihang University, China)

Detection of Hate Tweets using Machine Learning and Deep Learning .751
Lida Ketsbaia (Northumbria University, UK), Biju Issac (Northumbria University, UK), and Xiaomin Chen (Northumbria University, UK)

Use of Bash History Novelty Detection for Identification of Similar Source Attack Generation .759
Jack Hance (North Dakota State University, USA) and Jeremy Straub (Institute for Cyber Security Education and Research, North Dakota State University, USA)

Measurement Unit Placement Against Injection Attacks for the Secured Operation of an IIoT-Based Smart Grid .767
Adnan Anwar (Deakin University, Australia) and S. M. Abu Adnan Abir (IGW Operators Forum (IOF), Bangladesh)

Cross Platform IoT-Malware Family Classification Based on Printable Strings .775
Yen-Ting Lee (National Taiwan University of Science and Technology, Taiwan), Tao Ban (National Institute of Information and Communications Technology, Japan), Tzu-Ling Wan (National Taiwan University of Science and Technology, Taiwan), Shin-Ming Cheng (National Taiwan University of Science and Technology, Taiwan; Academia Sinica, Taiwan), Ryoichi Isawa (National Institute of Information and Communications Technology, Japan), Takeshi Takahashi (National Institute of Information and Communications Technology, Japan), and Daisuke Inoue (National Institute of Information and Communications Technology, Japan)

ALBFL: A Novel Neural Ranking Model for Software Fault Localization via Combining Static and Dynamic Features .785
Yuqing Pan (University of International Business and Economics, China; Tsinghua University, China), Xi Xiao (Tsinghua University, China; Peng Cheng Laboratory, China), Guangwu Hu (Shenzhen Institute of Information Technology, China), Bin Zhang (Peng Cheng Laboratory, China), Qing Li (Peng Cheng Laboratory, China; Southern University of Science and Technology, China), and Haitao Zheng (Tsinghua University, China)

Towards a Robust Classifier: An MDL-Based Method for Generating Adversarial Examples .793
Behzad Asadi (The University of Newcastle, Australia) and Vijay Varadharajan (The University of Newcastle, Australia)

Avoiding Geographic Regions in Tor .802
Matthew J. Ryan (Deakin University, Australia), Morshed Chowdhury (Deakin University, Australia), Frank Jiang (Deakin University, Australia), and Robin Ram Doss (Deakin University, Australia)

Identifying Cross-Version Function Similarity Using Contextual Features .810
Paul Black (Federation University, Australia), Iqbal Gondal (Federation University, Australia), Peter Vamplew (Federation University, Australia), and Arun Lakhotia (University of Louisiana at Lafayette, USA)

Scalable and Accurate Binary Code Search Method Based on Simhash and Partial Trace .818
Yunan Zhang (Guangdong Provincial Key Laboratory of Power System Network Security, Electric Power Research Institute, CSG, China), Aidong Xu Xu (Guangdong Provincial Key Laboratory of Power System Network Security, Electric Power Research Institute, CSG, China), and Yixin Jiang (Guangdong Provincial Key Laboratory of Power System Network Security, Electric Power Research Institute, CSG, China)

An Analytics Framework for Heuristic Inference Attacks Against Industrial Control Systems .827
Taejun Choi (The University of Queensland, Australia), Guangdong Bai (The University of Queensland, Australia), Ryan K L Ko (The University of Queensland, Australia), Naipeng Dong (The University of Queensland, Australia), Wenlu Zhang (The University of Queensland, Australia), and Shunyao Wang (The University of Queensland, Australia)

Forensic Analysis of Dating Applications on Android and iOS Devices .836
Shinelle Hutchinson (Purdue University, West Lafayette, IN), Neesha Shantaram (Purdue University, West Lafayette, IN), and Umit Karabiyik (Purdue University, West Lafayette, IN)

Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications .848
Nour Moustafa (University of New South Wales Canberra, Australia), Marwa Keshky (University of New South Wales Canberra, Australia), Essam Debiez (University of New South Wales Canberra, Australia), and Helge Janicke (Cyber Security Cooperative Research Centre, Edith Cowan University, Australia)

Privacy-Encoding Models for Preserving Utility of Machine Learning Algorithms in Social Media .856
Sara Salim (University of New South Wales, Australia), Nour Moustafa (University of New South Wales, Australia), and Benjamin Turnbull (University of New South Wales, Australia)

ETT - Emerging Technologies Track

Generation of Malicious Webpage Samples Based on GAN .864
Mengxiang wan (Wuhan University of Technology, China), Hanbing Yao (Wuhan University of Technology, China; Hubei Key Laboratory of Transportation Internet of Things, China), and Xin Yan (Wuhan University of Technology, China; Hubei Key Laboratory of Transportation Internet of Things, China)

A Flexible Attentive Temporal Graph Networks for Anomaly Detection in Dynamic Networks .870
Dali Zhu (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, Beijing, China), Yuchen Ma (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, Beijing, China), and Yinlong Liu (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, Beijing, China)

FPGA Based Blockchain System for Industrial IoT .876
Lei Xu (University of Texas Rio Grande Valley, US), Lin Chen (Texas Tech University, US), Zhimin Gao (Auburn University at Montgomery, US), Hanyee Kim (Korea University, Korea), Taeweon Suh (Korea University, Korea), and Weidong Shi (University of Houston, US)

Address-Based Signature .884
Handong Cui (The University of Hong Kong, Hong Kong) and Tsz Hon Yuen (The University of Hong Kong, Hong Kong)

Cryptanalysis of a Chaos-Based Block Cryptosystem Using Multiple Samples Correlation Power Analysis .892
Shunsheng Zhang (Guangxi Normal University, China), Yuling Luo (Guangxi Normal University, China; Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, China), Lvchen Cao (Guangxi Normal University, China), and Junxiu Liu (Guangxi Normal University, China)

Adversarial Attacks on Time-Series Intrusion Detection for Industrial Control Systems .899
Giulio Zizzo (Institute for Security Science and Technology; Department of Computing), Chris Hankin (Institute for Security Science and Technology; Department of Computing), Sergio Maffeis (Department of Computing), and Kevin Jones (Airbus)

Netspot: A Simple Intrusion Detection System with Statistical Learning .911
Alban Siffer (Amossys, Univ. Rennes, CNRS, IRISA), Pierre-Alain Fouque (Univ. Rennes, CNRS, IRISA), Alexandre Termier (Univ. Rennes, Inria, CNRS, IRISA), and Christine Largouet (AgroCampus Ouest, Inria, CNRS, IRISA)

Cache Side-Channel Attacks Detection Based on Machine Learning .919
Zhongkai Tong (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ziyuan Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhanpeng Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Limin Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yusha Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Yuxin Liu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

Exploit Internal Structural Information for IoT Malware Detection Based on Hierarchical Transformer Model 927
Xiaohui Hu (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Science, China), Rui Sun (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Science, China), Kejia Xu (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Science, China), Yongzheng Zhang (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Science, China), and Peng Chang (Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Science, China)

Inference Attacks on Physical Layer Channel State Information 935
Paul Walther (Chair for Privacy and Security, TU Dresden, Germany) and Thorsten Strufe (Karlsruhe Institute of Technology (KIT) and Centre for Tactile Internet, TU Dresden (CeTI))

A non-Discriminatory Approach to Ethical Deep Learning 943
Enzo Tartaglione (University of Torino, Italy) and Marco Grangetto (University of Torino, Italy)

Security and Privacy Implementation in Smart Home: Attributes Based Access Control and Smart Contracts 951
Amjad Qashlan (University of Technology Sydney(UTS), Australia), Priyadarsi Nanda (University of Technology Sydney (UTS), Australia), and Xiangjian He (University of Technology Sydney(UTS), Australia)

Blockchain-Based Verifiable Credential Sharing with Selective Disclosure 959
Rahma Mukta (University of New South Wales (UNSW Sydney), Sydney), James Martens (University of New South Wales (UNSW Sydney), Sydney), Hye-young Paik (University of New South Wales (UNSW Sydney), Sydney), Qinghua Lu (Data61, CSIRO, Sydney), and Salil S. Kanhere (University of New South Wales (UNSW Sydney), Sydney)

Blockchain-Enabled Collaborative Intrusion Detection in Software Defined Networks 967
Wenjun Fan (University of Colorado Colorado Springs, United States), Younghee Park (San Jose State University, United States), Shubham Kumar (San Jose State University, United States), Priyatham Ganta (San Jose State University, United States), Xiaobo Zhou (University of Colorado Colorado Springs, United States), and Sang-Yoon Chang (University of Colorado Colorado Springs, United States)

Active DNN IP Protection: A Novel User Fingerprint Management and DNN Authorization Control Technique 975
Mingfu Xue (Collaborative Innovation Center of Novel Software Technology and Industrialization, China; Nanjing University of Aeronautics and Astronautics, China), Zhiyu Wu (Nanjing University of Aeronautics and Astronautics, China), Can He (Collaborative Innovation Center of Novel Software Technology and Industrialization, China; Nanjing University of Aeronautics and Astronautics, China), Jian Wang (Collaborative Innovation Center of Novel Software Technology and Industrialization, China; Nanjing University of Aeronautics and Astronautics, China), and Weiqiang Liu (Nanjing University of Aeronautics and Astronautics, China)

SCPORAM: A Hardware Support Scheme for Protecting Memory Access Patterns .983
Zhanpeng Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ziyuan Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Limin Wang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhongkai Tong (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Chao Yan (Institute of Information Engineering, Chinese Academy of Sciences, China)

QPBFT: Practical Byzantine Fault Tolerance Consensus Algorithm Based on Quantified-Role .991
Zhujun Zhang (Institute of Information Engineering, Chinese Academy of Sciences, University of Chinese Academy of Sciences, China), Dali Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China), and Wei Fan (Institute of Information Engineering, Chinese Academy of Sciences, China)

Privacy-Preserving Public Verification of Ethical Cobalt Sourcing .998
Kilian Becher (Chair of Privacy and Data Security, TU Dresden, Germany), J. A. Gregor Lagodzinski (Hasso Plattner Institute, University of Potsdam, Germany), and Thorsten Strufe (Chair of IT Security, Karlsruhe Institute of Technology, Germany)

A Computation Offloading Model over Collaborative Cloud-Edge Networks with Optimal Transport Theory .1006
Zhuo Li (Computer Network Information Center, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xu Zhou (Computer Network Information Center, Chinese Academy of Sciences, China), Yang Liu (Beijing Normal University, China), Congshan Fan (Computer Network Information Center, Chinese Academy of Sciences, China), and Wei Wang (Knet Technologies Co. Ltd., China)

A Secure Shard Reconfiguration Protocol for Sharding Blockchains Without a Randomness .1012
Yizhong Liu (Beihang University, China), Jianwei Liu (Beihang University, China), Yiming Hei (Beihang University, China), Wei Tan (Xidian University, China), and Qianhong Wu (Beihang University, China)

Revocable and Offline-Verifiable Self-Sovereign Identities .1020
Andreas Abraham (Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology, Graz, Austria), Stefan More (Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology, Graz, Austria), Christof Rabensteiner (Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology, Graz, Austria), and Felix Hörandner (Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology, Graz, Austria)

Blockchain Based End-to-End Tracking System for Distributed IoT Intelligence Application Security Enhancement .1028
Lei Xu (University of Texas Rio Grande Valley, USA), Zhimin Gao (Auburn University at Montgomery, USA), Xinxin Fan (IoTeX, USA), Lin Chen (Texas Tech University, USA), Hanyee Kim (Korea University, Korea), Taeweon Suh (Korea University, Korea), and Weidong Shi (University of Houston, USA)

Time is Money: Countering Griefing Attack in Lightning Network .1036
Subhra Mazumdar (Cryptology and Security Research Unit, Indian Statistical Institute, India), Prabal Banerjee (Cryptology and Security Research Unit, Indian Statistical Institute, India), and Sushmita Ruj (CSIRO, Data61, Australia; Cryptology and Security Research Unit, Indian Statistical Institute, India)

Preventing a Fork in a Blockchain - David Fighting Goliath .1044
Przemysław Kubiak (Wrocław University of Science and Technology, Wrocław, Poland) and Mirosław Kutyłowski (Wrocław University of Science and Technology)

Golden-Chip-Free Hardware Trojan Detection Through Thermal Radiation Comparison in Vulnerable Areas .1052
Ting Su (National University of Defense Technology, China), Jiahe Shi (National University of Defense Technology, China), Yongkang Tang (National University of Defense Technology, China), and Shaoqing Li (National University of Defense Technology, China)

A Feedback-Driven Lightweight Reputation Scheme for IoV .1060
Rohan Dahiya (Deakin University, Australia), Frank Jiang (Deakin University, Australia), and Robin Ram Doss (Deakin University, Australia)

Modelling Attacks in Blockchain Systems using Petri Nets .1069
Md. Atik Shahriar (Shahjalal University of Science & Technology, Bangladesh), Faisal Haque Bappy (Shahjalal University of Science and Technology, Bangladesh), A. K. M. Fakhrul Hossain (Shahjalal University of Science and Technology, Bangladesh), Dayamoy Datta Saikat (Shahjalal University of Science and Technology, Bangladesh), Md Sadek Ferdous (Shahjalal University of Science and Technology, Bangladesh; Imperial College London, UK), Mohammad Jabed M. Chowdhury (La Trobe University, Australia), and Md Zakirul Alam Bhuiyan (Fordham University, USA)

BONIK: A Blockchain Empowered Chatbot for Financial Transactions .1079
Md. Saiful Islam Bhuiyan (Shahjalal University of Science and Technology, Bangladesh), Abdur Razzak (Shahjalal University of Science and Technology, Bangladesh), Md Sadek Ferdous (Shahjalal University of Science and Technology, Bangladesh; Imperial College London, United Kingdom), Mohammad Jabed M. Chowdhury (La Trobe University, Australia), Mohammad A. Hoque (University of Helsinki, Finland), and Sasu Tarkoma (University of Helsinki, Finland)

Towards Network Traffic Monitoring Using Deep Transfer Learning .1089
Harsh Dhillon (Western University, Canada) and Anwar Haque (Western University, Canada)

The Work-in-Progress (WiP) Track of the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020)

Session WiP-1

A Three-Stage Machine Learning Network Security Solution for Public Entities .1097
Stanisław Saganowski (Wroclaw University of Science and Technology, Poland)

Multi-input Functional Encryption: Efficient Applications from Symmetric Primitives .1105
Alexandros Bakas (Tampere University, Finland) and Antonis Michalas (Tampere University, Finland)

Factors Affecting Users' Disclosure Decisions in Android Runtime Permissions Model .1113
Rawan Baalous (University of Glasgow, United Kingdom) and Ronald Poet (University of Glasgow, United Kingdom)

Towards a Lightweight Continuous Authentication Protocol for Device-to-Device Communication .1119
Syed Wajid Ali Shah (Deakin University, Australia), Naeem Firdous Syed (Deakin University, Australia), Arash Shaghaghi (Deakin University, Australia), Adnan Anwar (Deakin University, Australia), Zubair Baig (Deakin University, Australia), and Robin Doss (Deakin University, Australia)

Secure and Privacy Preserving Method for Biometric Template Protection using Fully Homomorphic Encryption .1127
Arun Kumar Jindal (Tata Consultancy Services, India), Imtiyazuddin Shaik (Tata Consultancy Services, India), Vasudha Vasudha (Tata Consultancy Services, India), Srinivasa Rao Chalamala (Tata Consultancy Services, India), Rajan Ma (Tata Consultancy Services, India), and Sachin Lodha (Tata Consultancy Services, India)

Trusted Network Slicing Among Multiple Mobile Network Operators .1135
Jehanzaib Yousuf Muhammad (State Key Lab of ISN, Xidian University, P.R.C), Mingjun Wang (State Key Lab of ISN, Xidian University, P.R.C), Zheng Yan (State Key Lab of ISN, Xidian University, P.R.C.; Aalto University, Finland), and Fawad Khan (National University of Sciences & Technology, Pakistan)

A Scoring System to Efficiently Measure Security in Cyber-Physical Systems .1141
Andreas Aigner (Landshut University of Applied Science, Germany) and Abdelmajid Khelil (Landshut University of Applied Science, Germany)

Towards a new Deep Learning Based Approach for the Password Prediction .1146
Manaz Kaleel (University College Dublin, Ireland) and Nhien-An Le-Khac (University College Dublin, Ireland)

DANTE: Predicting Insider Threat using LSTM on System Logs .1151
Nidhi Rastogi (Rensselaer Polytechnic Institute, USA) and Qicheng Ma (Rensselaer Polytechnic Institute, USA)

VGG-Based Side Channel Attack on RSA Implementation .1157
Qi Lei (Bank Card Test Center (BCTC), China), Chao Li (Bank Card Test Center (BCTC), China), Kexin Qiao (Bank Card Test Center (BCTC), China), Zhe Ma (Bank Card Test Center (BCTC), China), and Bo Yang (Bank Card Test Center (BCTC), China)

Deep Learning for Password Guessing and Password Strength Evaluation, A Survey .1162
Tao Zhang (Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, China; Guangxi Key Laboratory of Trusted Software, Guangxi University for Nationalities, China; Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis, Guangxi University for Nationalities, China), Zelei Cheng (Purdue University, USA), Yi Qin (Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, China), Qiang Li (PLA Information Engineering University, China; Henan Key Laboratory of Network Cryptography Technology, China), and Lin Shi (Cloud Computing and Big Data Research Institute, China Academy of Information and Communications Technology, China)

Metrics to Enhance the Resilience of Cyber-Physical Systems .1167
Michel Barbeau (Carleton University, Canada), Frédéric Cuppens (Ecole Polytechnique de Montréal, Canada), Nora Cuppens (Ecole Polytechnique de Montréal, Canada), Romain Dagnas (Institut de Recherche Technologique SystemX, France), and Joaquin Garcia-Alfaro (Institut Polytechnique de Paris, SAMOVAR, Telecom SudParis, France)

Independent Worker Selection In Crowdsourcing .1173
Ang Li (Hunan University, China), Wenjun Jiang (Hunan University, China), Xueqi Li (Hunan University, China), Xinrong Chen (Hunan University, China), and Guojun Wang (Guangzhou University, China)

Towards Collaborative Intrusion Detection Enhancement Against Insider Attacks with Multi-level Trust .1179
Wenjuan Li (Guangzhou University, China; Technical University of Denmark, Denmark), Weizhi Meng (Technical University of Denmark, Denmark), and Hui Zhu (Technical University of Denmark, Denmark)

A Function-Centric Risk Assessment Approach for Android Applications .1187
Min Li (Guangzhou University, China), Haroon Elahi (Guangzhou University, China), Tao Peng (Guangzhou University, China), Fang Qi (Central South University, China), and Guojun Wang (Guangzhou University, China)

SCAFFISD: A Scalable Framework for Fine-Grained Identification and Security Detection of Wireless Routers .1194
Fangzhou Zhu (Nanjing University of Aeronautics and Astronautics, China), Liang Liu (Nanjing University of Aeronautics and Astronautics, China), Weizhi Meng (Technical University of Denmark, Denmark), Ting Lv (Nanjing University of Aeronautics and Astronautics, China), Simin Hu (Nanjing University of Aeronautics and Astronautics, China), and Renjun Ye (Nanjing University of Aeronautics and Astronautics, China)

Library Implementation and Performance Analysis of GlobalPlatform TEE Internal API for Intel SGX and RISC-V Keystone .1200
Kuniyasu Suzaki (Technology Research Association of Secure IoT Edge application based on RISC-V Open architecture (TRASIO); National Institute of Advanced Industrial Science and Technology (AIST)), Kenta Nakajima (Technology Research Association of Secure IoT Edge application based on RISC-V Open architecture (TRASIO)), Tsukasa Oi (Technology Research Association of Secure IoT Edge application based on RISC-V Open architecture (TRASIO)), and Akira Tsukamoto (National Institute of Advanced Industrial Science and Technology (AIST))

A Privacy-Preserving Data Inference Framework for Internet of Health Things Networks .1209
James Jin Kang (Edith Cowan University, Australia), Mahdi Dibaei (Islamic Azad University Tabriz Branch, Iran), Gang Luo (Macquarie University, Australia), Wencheng Yang (Edith Cowan University, Australia), and Xi Zheng (Macquarie University, Australia)

RPAD: An Unsupervised HTTP Request Parameter Anomaly Detection Method .1215
Yizhen Sun (State Grid Information & Communication Company of Hunan Electric Power Corporation, P. R. China), Yiman Xie (Central South University, P. R. China), Weiping Wang (Central South University, P. R. China), Shigeng Zhang (Central South University, P. R. China), Yuxi Wu (State Grid Information & Communication Company of Hunan Electric Power Corporation, P. R. China), and Jingchuan Feng (State Grid Information & Communication Company of Hunan Electric Power Corporation, P. R. China)

Image Self-Recovery Based on Authentication Feature Extraction .1222
Tong Liu (Faculty of Information Technology, Macau University of Science and Technology, China) and Xiaochen Yuan (Faculty of Information Technology, Macau University of Science and Technology, China; Zhuhai MUST Science & Technology Research Institute, China)

Do My Emotions Influence What I Share? Analysing the Effects of Emotions on Privacy Leakage in Twitter .1228
Manasi Mittal (The University of Auckland, New Zealand), Muhammad Rizwan Asghar (The University of Auckland, New Zealand), and Arvind Tripathi (The University of Auckland, New Zealand)

Robustness Analysis and Defence Strategy of an Interdependent Networks Model Based on Closeness Centrality .1236
Jinfang Sheng (Central South University, Changsha, China), Yan Hu (Central South University, Changsha, China), Kerong Guan (Central South University, Changsha, China), Bin Wang (Central South University, Changsha, China), Xiaoxia Pan (Central South University, Changsha, China), and Wenjun Kang (Central South University, Changsha, China)

A Framework for Measuring IoT Data Quality Based on Freshness Metrics .1242
Fatma Mohammed (La Trobe University, Australia), A. S. M. Kayes (La Trobe University, Australia), Eric Pardede (La Trobe University, Australia), and Wenny Rahayu (La Trobe University, Australia)

RevBloc: A Blockchain-Based Secure Customer Review System .1250
Xiuli Fang (The University of Auckland, New Zealand) and Muhammad Rizwan Asghar (The University of Auckland, New Zealand)

Face2Face Manipulation Detection Based on Histogram of Oriented Gradients .1260
Amr Megahed (Harbin Institute of Technology, China) and Qi Han (Harbin Institute of Technology, China)

Analysis and Modelling of Multi-stage Attacks .1268
Saurabh Chamotra (Cyber Security Technology Division, India) and Ferdous Ahmed Barbhuiya (Indian Institute of Information Technology (IIIT Guwahati), India)

Cyber Situation Awareness Monitoring and Proactive Response for Enterprises on the Cloud .1276
Hootan Alavizadeh (Imam Reza International University, Iran), Hooman Alavizadeh (Massey University, New Zealand), and Julian Jang-Jaccard (Massey University, New Zealand)

Explicitly Privacy-Aware Space Usage Analysis .1285
Sanjiv S. Jha (Institute of Computer Science, University of St. Gallen, Switzerland), Simon Mayer (Institute of Computer Science, University of St. Gallen, Switzerland), and Tanja Schneider (Technology Studies, University of St. Gallen, Switzerland)

Towards a Transparent and Privacy-Preserving Healthcare Platform with Blockchain for Smart Cities .1291
Abdullah Al Omar (University of Asia Pacific, Bangladesh), Abu Kaisar Jamil (University of Asia Pacific, Bangladesh), Shakhawath Hossain Nur (University of Asia Pacific, Bangladesh), Mahamudul Hasan (University of Asia Pacific, Bangladesh), Rabeya Bosri (Fordham University, USA), Zakirul Alam Bhuiyan (University of Liberal Arts Bangladesh, Bangladesh), and Mohammad Shahriar Rahman (University of Liberal Arts Bangladesh, Bangladesh)

BML: A Data Mapping Language for Blockchain Platforms .1297
Ba-Lam Do (Hanoi University of Science and Technology, Vietnam), Quang-Thang Nguyen (Hanoi University of Science and Technology, Vietnam), Thang Nguyen (Hanoi University of Science and Technology, Vietnam), Tien-Thao Nguyen (Hanoi University of Science and Technology, Vietnam), Thanh-Chung Dao (Hanoi University of Science and Technology, Vietnam), and BinhMinh Nguyen (Hanoi University of Science and Technology, Vietnam)

The 11th International Workshop on Collaborative Computing with Cloud and Client (C4W 2020)

Session C4W-1

Semantic Location Privacy Protection Algorithm Based on Edge Cluster Graph .1304
Tao Lu (South China University of Technology, China), Hongyun Xu (South China University of Technology, China), Kai Tian (South China University of Technology, China), Cenxi Tian (South China University of Technology, China), and Rui Jiang (South China University of Technology, China)

Priority Based Modeling and Comparative Study of Google Cloud Resources between 2011 and 2019 .1310
Dimuth Lasantha (Centre for Intelligent Systems (CIS), Central Queensland University, Rockhampton, Australia) and Biplob Ray (Centre for Intelligent Systems (CIS), Central Queensland University, Rockhampton, Australia)

Security Challenges and Solutions for 5G HetNet .1318
Aakanksha Sharma (Federation University, Australia), Venki Balasubramanian (Federation University, Australia), and Alireza Jolfaei (Macquarie University, Australia)

Privacy Smells: Detecting Privacy Problems in Cloud Architectures .1324
Immanuel Kunz (Fraunhofer AISEC, Germany), Angelika Schneider (Fraunhofer AISEC, Germany), and Christian Banse (Fraunhofer AISEC, Germany)

BlockSLAP: Blockchain-Based Secure and Lightweight Authentication Protocol for Smart Grid .1332
Weizheng Wang (The University of Aizu, Japan), Huakun Huang (The University of Aizu, Japan), Lejun Zhang (Yangzhou University, China), Zhaoyang Han (The University of Aizu, Japan), Chen Qiu (The University of Aizu, Japan), and Chunhua Su (The University of Aizu, Japan)

SecureESFS: Sharing Android External Storage Files in a Securer Way .1339
Shan Liang (State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China; University of Chinese Academy of Sciences, China), Yuewu Wang (State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China; University of Chinese Academy of Sciences, China), Lingguang Lei (State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China; University of Chinese Academy of Sciences, China), Jiwu Jing (University of Chinese Academy of Sciences, China), and Quan Zhou (State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China)

PPFQ: Privacy-Preserving Friends Query over Online Social Networks .1348
Yuxi Li (Northeastern University, China), Fucai Zhou (Northeastern University, China), and Zifeng Xu (Northeastern University, China)

Dynamic flow Redirecton Scheme for Enhancing Control Plane Robustness in SDN .1354
Dong Liang (Information Engineering University, China), Qinrang Liu (Information Engineering University, China), Yanbin Hu (Information Engineering University, China), Tao Hu (Information Engineering University, China), Binghao Yan (Information Engineering University, China), and Haiming Zhao (State Key Laboratory of Astronautic Dynamics, China)

Prov-IoT: A Security-Aware IoT Provenance Model .1360
Fariha Tasmin Jaigirdar (Monash University, Australia), Carsten Rudolph (Monash University, Australia), and Chris Bain (Monash University, Australia)

Are Smart Home Devices Abandoning IPV Victims? .1368
Ahmed Alshehri (Colorado School of Mines, USA), Malek Ben Salem (Accenture Labs, USA), and Lei Ding (American University, D.C., USA)

A Practical Privacy-Preserving Algorithm for Document Data .1376
Tomoaki Mimoto (KDDI Research, Inc., Japan), Shinsaku Kiyomoto (KDDI Research, Inc., Japan), Koji Kitamura (National Institute of Advanced Industrial Science and Technology, Japan), and Atsuko Miyaji (Osaka University, Japan)

TORP: Load Balanced Reliable Opportunistic Routing for Asynchronous Wireless Sensor Networks .1384
Muhammad Umar Farooq Qaisar (University of Science and Technology of China, China), Xingfu Wang (University of Science and Technology of China, China), Ammar Hawbani (University of Science and Technology of China, China), Asad Khan (Guangzhou University, China), Adeel Ahmed (University of Science and Technology of China, China), and Fisseha Teju Wedaj (University of Science and Technology of China, China)

CPN Model Checking Method of Concurrent Software Based on State Space Pruning .1390
Tao Sun (Inner Mongolia University, China), Jing Yang (Inner Mongolia University, China), and Wenjie Zhong (Inner Mongolia University, China)

An Arithmetic Differential Privacy Budget Allocation Method for the Partitioning and Publishing of Location Information .1395
Yan Yan (Lanzhou University of Technology, China; Macquarie University, Australia), Xin Gao (Lanzhou University of Technology, China), Adnan Mahmood (Macquarie University, Australia; Telecommunications Software and Systems Group, Republic of Ireland), Yang Zhang (Wuhan University, China; Macquarie University, Australia), Shuang Wang (Southeast University, China; Macquarie University, Australia), and Quan Z. Sheng (Macquarie University, Australia)

IoT-Sphere: A Framework to Secure IoT Devices from Becoming Attack Target and Attack Source .1402
Syed Ghazanfar Abbas (University of Engineering and Technology, Pakistan), Muhammad Husnain (University of Engineering and Technology, Pakistan), Ubaid Ullah Fayyaz (University of Engineering and Technology, Pakistan), Farrukh Shahzad (University of Engineering and Technology, Pakistan), Ghalib A. Shah (University of Engineering and Technology, Pakistan), and Kashif Zafar (National University of Computer and Emerging Sciences, Pakistan)

Membership Inference Attacks: Analysis and Mitigation .1410
Md Shamimur Rahman Shuvo (University of New Brunswick, Canada) and Dima Alhadidi (University of Windsor, Canada)

Bearicade: Secure Access Gateway to High Performance Computing Systems .1420
Taha Al-Jody (University of Huddersfield, UK), Violeta Holmes (University of Huddersfield, UK), Alexandros Antoniades (University of Huddersfield, UK), and Yazan Kazkouzeh (University of Huddersfield, UK)

Enhancing Cyber Security Using Audio Techniques: A Public Key Infrastructure for Sound .1428
Anthony Phipps (Cyber Security Research Centre, London Metropolitan University, UK), Karim Ouazzane (Cyber Security Research Centre, London Metropolitan University, UK), and Vassil Vassilev (Cyber Security Research Centre, London Metropolitan University, UK)

Group Communication Needs No Consistent Transcript Distribution .1437
Klaus Herberth (University of Konstanz, Germany)

Name-Signature Lookup System: A Security Enhancement to Named Data Networking .1444
Zhicheng Song (University of Nottingham, United Kingdom) and Pushpendu Kar (University of Nottingham Ningbo China, China)

Feature Importance in Android Malware Detection .1449
Vasileios Kouliaridis (University of the Aegean, Greece), Georgios Kambourakis (European Commission, Joint Research Centre, Italy), and Tao Peng (Guangzhou University, China)

iTES: Integrated Testing and Evaluation System for Software Vulnerability Detection Methods .1455
Chi Zhang (Jiangsu University, China), Jinfu Chen (Jiangsu University, China), Saihua Cai (Jiangsu University, China), Bo Liu (Jiangsu University, China), Yiming Wu (Jiangsu University, China), and Ye Geng (Jiangsu University, China)

The 10th International Workshop on Assistive Engineering and Information Technology (AEIT 2020)

Session AEIT-1

Plant Taxonomy in Hainan Based on Deep Convolutional Neural Network and Transfer Learning 1461
Wei Liu (Hainan Medical University, China), Wenlong Feng (Hainan University, China), Mengxing Huang (Hainan University, China), Guilai Han (Hainan Medical University, China), and Jialun Lin (Hainan Medical University, China)

Research on Stitching and Alignment of Mouse Carcass EM Images .1468
Jing Zhu (Soochow University, China), Hongyu Ge (Soochow University, China), Ao Cheng (Soochow University, China), Ruobing Zhang (Suzhou institute of biomedical engineering and technology Chinese academy of science, China), and Lirong Wang (Soochow University, China)

A Simple Analysis of Multimodal Data Fusion .1472
Jiangchang Cheng (Hunan Normal University, China), Yinglong Dai (Hunan Provincial Key Laboratory of Intelligent Computing and Language Information Processing, Hunan Normal University, China; National University of Defense Technology, China), Yao Yuan (Hunan Normal University, China), and Hongli Zhu (Hunan Normal University, China)

Pyramid Pooling Channel Attention Network for Esophageal Tissue Segmentation on OCT Images..... 1476
Deyin Li (Soochow University, China), Miao Zhang (Soochow University, China), Wei Shi (Soochow University, China), Huimin Zhang (Soochow University, China), Duoduo Wang (Soochow University, China), and Lirong Wang (Soochow University, China)

Atrial Fibrillation Classification Using Convolutional Neural Networks and Time Domain Features of ECG Sequence .1481
Dong Wang (Soochow University, China), Lishen Qiu (Rehabilitation department Suzhou institute of biomedical, engineering and technology Chinese academy of science, China), Wei Shi (Soochow University, China), Hongqing Wang (Soochow University, China), Xiangxiang Xu (Soochow University, China), and Lirong Wang (Soochow University, China)

Design and Implementation of a Multifunctional ECG Analysis Software System .1486
Dong Wang (Soochow University, China), Lishen Qiu (Chinese Academy of Sciences, China), Wei Shi (Soochow University, China), Hongqing Wang (Soochow University, China), and Xiangxiang Xu (Soochow University, China)

A Four-Feature Keyword Extraction Algorithm Based on Word Length Priority Ratio .1492
Hui Kang (Jilin University, China), Lingfeng Lu (Jilin university, China), and Hang Su (Tool product platform department, AVIC China Aero-Poly technology Establishment, China)

Research and Improvement of Community Discovery Algorithm Based on Spark for Large Scale Complicated Networks .1499
Hui Kang (Jilin University), ShengQuan Chen (Jilin University), Lingfeng Lu (Jilin University), and ChenKun Meng (Jilin University)

An Investigation of Assistive Products for the Elderly .1509
Xiaoying Li (Nagasaki Institute of Applied Science, Japan; Faculty of Artistic Designing), Huaibin Wang (Tianjin University of Technology, China), Yuqiong Liu (Zhejiang University of Technology, China), Yuefei Wang (Nagasaki Institute of Applied Science, Japan; Advanced Institute of Science and Technology, BeiBu Gulf University, China), and Zhen Liu (Nagasaki Institute of Applied Science, Japna; Tianjin University of Technology, China)

An Impedance Control Method of Lower Limb Exoskeleton Rehabilitation Robot Based on Predicted Forward Dynamics .1515
Yuefei Wang (Nagasaki Institute of Applied Science, Japan; Institute of Advanced Science and Technology, Beibu Gulf University, China), Zhen Liu (Nagasaki Institute of Applied Science, Japan; Institute of Advanced Science and Technology, Beibu Gulf University, China), Liucun Zhu (Institute of Advanced Science and Technology, Beibu Gulf University, China), Xiaoying Li (Nagasaki Institute of Applied Science, Japan), and Huaibin Wang (Tianjin University of Technology, China)

An Automatic Vulnerability Scanner for Web Applications .1519
Haibo Chen (Jiangsu University, China), Junzuo Chen (Jiangsu University, China), Jinfu Chen (Jiangsu University, China), Shang Yin (Jiangsu University, China), Yiming Wu (Jiangsu University, China), and Jiaping Xu (Jiangsu University, China)

An Automatic Vulnerability Classification System for IoT Softwares .1525
Haibo Chen (Jiangsu University, China), Dalin Zhang (Jiangsu University, China), Jinfu Chen (Jiangsu University, China), Wei Lin (Jiangsu University, China), Dengzhou Shi (Jiangsu University, China), and Zian Zhao (Jiangsu University, China)

The 5th International Workshop on Privacy, Data Assurance, Security Solutions in the Internet of Things (PASS4IoT 2020)

Session PASS4IoT-1

Policy Evaluation and Dynamic Management Based on Matching Tree for XACML .1530
Hongzhaoning Kang (XIDIAN University, China), Liu Gang (XIDIAN University, China), Quan Wang (XIDIAN University, China), Runnan Zhang (XIDIAN University, China), Zichao Zhong (XIDIAN University, China), and Yumin Tian (XIDIAN University, China)

Fined-Grained Aspect Extraction from Online Reviews for Decision Support .1536
Zhaoli Liu (Xi'an University of Technology, China), Qindong Sun (Xi'an University of Technology, China), Zhihai Yang (Xi'an University of Technology, China), Kun Jiang (Xi'an University of Technology, China), and Jinpei Yan (Xi'an University of Technology, China)

A Password Strength Evaluation Algorithm Based on Sensitive Personal Information .1542
Xinchun Cui (Qufu Normal University, China; Guangxi Key Laboratory of Cryptography and Information Security, China), Comxueqing Li (Qufu Normal University, China), Yiming Qin (Qufu Normal University, China), and Yong Ding (Guangxi Key Laboratory of Cryptography and Information Security, China)

Prediction of high Precision Ignition Process in the Condition of Multi Flow Area Coupling of Micro Solid Rocket Motor .1546
Gaofei Wei (Northwestern Polytechnical University, China), Qiang Cai (China Academy of Launch Vehicle Technology, China), Meng Li (Xi'an Modern Chemistry Research Institute, China), Rui Dong (Northwestern Polytechnical University, China), and Yang Liu (Northwestern Polytechnical University, China)

The 4th International Workshop on Cyberspace Security (IWCSS 2020)

Session IWCSS-1

Exploiting User Selection Algorithm for Securing Wireless Communication Networks .1552
Xiaoying Qiu (Beijing Information Science and Technology University, China), Guangda Li (Beijing Information Science and Technology University, China), Xuan Sun (Beijing Information Science and Technology University, China), and Zhiguo Du (People's Public Security University of China, China)

Easy-to-Implement Campus Electronic Anonymous Voting System .1556
Zhang Ruxian (Beijing University of Posts and Telecommunications, China; University of International Relations, China), Zhang Zhaoju (University of International Relations, China), and Di Hong (University of International Relations, China)

Hypergraph Attention Networks .1560
Chaofan Chen (University of Science and Technology of China, China), Zelei Cheng (Purdue University, USA), Zuotian Li (Carnegie Mellon University, USA), and Manyi Wang (Beijing University of Posts and Telecommunications, China)

Search & Catch: Detecting Promotion Infection in the Underground through Search Engines .1566
Ronghai Yang (Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China; Sangfor Technologies Co., Ltd), Jia Liu (Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China), Liang Gu (Sangfor Technologies Co., Ltd), and Yurong Chen (Beijing University of Posts and Telecommunications)

Image Authentication Using QR Code Watermarking Approach Based on Image Segmentation .1572
Xiaomei Liu (University of International Relations, China) and Xin Tang (University of International Relations, China)

A Semi-Supervised Learning Scheme to Detect Unknown DGA Domain Names Based on Graph Analysis .1578
Fan Yan (Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences & Sangfor Inc., China), Jia Liu (Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China), Liang Gu (Sangfor Inc., China), and Zelong Chen (University of Jinan Quancheng College, China)

A PHP and JSP Web Shell Detection System with Text Processing Based on Machine Learning .1584
Han Zhang (Shanghai Jiao Tong University, China), Ming Liu (Shanghai Jiao Tong University, China), Zihan Yue (Shanghai Jiao Tong University, China), Zhi Xue (Shanghai Jiao Tong University, China), Yong Shi (Shanghai Jiao Tong University, China), and Xiangjian He (University of Technology Sydney, Australia)

A Symmetric Uniform Formula and Sole Index Method for Sieving (Twin) Primes .1592
Wei Ren (China University of Geosciences, China; Guangxi Key Laboratory of Cryptography and Information Security, China; Key Laboratory of Network Assessment Technology, CAS, Institute of Information Engineering, Chinese Academy of Sciences, China)

SCScan: A SVM-Based Scanning System for Vulnerabilities in Blockchain Smart Contracts .1598
Xiaohan Hao (China University of Geoscience, China), Wei Ren (China University of Geoscience, China), Wenwen Zheng (China University of Geoscience, China), and Tianqing Zhu (China University of Geoscience, China)

A Security Model and Implementation of Embedded Software Based on Code Obfuscation .1606
Jiajia Yi (University of Electronic Science and Technology of China, China), Lirong Chen (University of Electronic Science and Technology of China, China), Haitao Zhang (University of Electronic Science and Technology of China, Shanghai Automotive Industry Corporation Technology Center, China), Yun Li (Guangdong Weichen Information Technology Co., Ltd, China), and Huanyu Zhao (Guangdong Weichen Information Technology Co., Ltd, China)

Sensitive Information Detection Based on Convolution Neural Network and Bi-Directional LSTM .1614
Yan Lin (Beijing University of Posts and Telecommunications, China), Guosheng Xu (Beijing University of Posts and Telecommunications, China), Guoai Xu (Beijing University of Posts and Telecommunications, China), Yudong Chen (Beijing University of Posts and Telecommunications, China), and Dawei Sun (Beijing Softsec Technology Co., Ltd., China)

Enhancing the Security of Numeric Comparison Secure Simple Pairing in Bluetooth 5.0 .1622
Dongkun Hou (Xi'an Jiaotong-Liverpool University, China), Jie Zhang (Xi'an Jiaotong-Liverpool University, China), and Ka Lok Man (Xi'an Jiaotong-Liverpool University, China)

3P3: Strong Flexible Privacy for Broadcasts .1630
David Mödinger (Institute of Distributed Systems, Ulm University) and Franz J. Hauck (Institute of Distributed Systems, Ulm University)

Efficient Revocable Attribute-Based Encryption with Hidden Policies .1638
Dominik Ziegler (Know-Center GmbH, Austria) and Alexander Marsalek (IAIK, Graz University of Technology, Austria)

On the Usefulness of User Nudging and Strength Indication Concerning Unlock Pattern Security .1646
Thomas Hupperich (University Münster, Germany) and Katharina Dassel (University Münster, Germany)

Unbounded Key-Policy Attribute-Based Encryption with Black-Box Traceability .1655
Yunxiu Ye (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China), Zhenfu Cao (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China; Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen and Shanghai Institute of Intelligent Science and Technology, Tongji University, China), and Jiachen Shen (Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, China)

An Efficient Vulnerability Extrapolation Using Similarity of Graph Kernel of PDGs .1664
Jingxiang Zeng (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xiaofan Nie (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Liwei Chen (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Jinfeng Li (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Gewangzi Du (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Gang Shi (Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

Opportunistic Tracking in Cyber-Physical Systems .1672
Samaneh Rashidibajgan (University Münster, Germany), Thomas Hupperich (University Münster, Germany), Robin Doss (Deakin University, Australia), and Lei Pan (Deakin University, Australia)

An Approach for Poisoning Attacks Against RNN-Based Cyber Anomaly Detection .1680……
Jinghui Xu (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Yu Wen (Institute of Information Engineering, Chinese Academy of Sciences, China), Chun Yang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), and Dan Meng (Institute of Information Engineering, Chinese Academy of Sciences, China)

Differential Privacy Images Protection Based on Generative Adversarial Network .1688……
Ren Yang (Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Inner Mongolia University, China), Xuebin Ma (Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Inner Mongolia University, China), Xiangyu Bai (Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Inner Mongolia University, China), and Xiangdong Su (Inner Mongolia University, China)

DP-Eclat:A Vertical Frequent Itemset Mining Algorithm Based on Differential Privacy .1696……
Shengyi Guan (Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Inner Mongolia University, China), Xuebin Ma (Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Inner Mongolia University, China), Wuyungerile Li (Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Inner Mongolia University, China), and Xiangyu Bai (Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing, Inner Mongolia University, China)

More Efficient SM9 Algorithm Based on Bilinear Pair Optimization Processing .1704……
Xianze Liu (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China; Security University of Chinese Academy of Sciences, China), Jihong Liu (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China; Security, University of Chinese Academy of Sciences, China), Bifei Jiang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China; Security, University of Chinese Academy of Sciences, China), Haozhen Jiang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China; Security, University of Chinese Academy of Sciences, China), and Zhi Yang (Beijing Trusted Huatai Information Technology Co., Ltd)

SeWG: Security-Enhanced WireGuard for Android Based on TEE .1711
Yongkang Wu (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, China), Yiwei Shan (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China), Zhichao Wang (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, China), Pengcheng Zhang (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, China), Min He (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, China), and Jihong Liu (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; University of Chinese Academy of Sciences, China)

Differential Privacy Preserving Data Publishing Based on Bayesian Network .1718
Xuejian Qi (Inner Mongolia University, China), Xuebin Ma (Inner Mongolia University, China), Xiangyu Bai (Inner Mongolia University, China), and Wuyungeril Li (Inner Mongolia University, China)

Implementing Network Attack Detection with a Novel NSSA Model Based on Knowledge Graphs 1727
Yixuan Wang (University of Electronic Science and Technology of China, China), Yujun Li (University of Electronic Science and Technology of China, China), Xiang Chen (University of Electronic Science and Technology of China, China), and Yeni Luo (University of Electronic Science and Technology of China, China)

UIDroid: User-Driven Based Hierarchical Access Control for Sensitive Information .1733
Luping Ma (Institute of Information Engineering, Chinese Academy of Sciences, China), Dali Zhu (Institute of Information Engineering, Chinese Academy of Sciences, China), Shunliang Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China), Xiaohui Zhang (Institute of Information Engineering, Chinese Academy of Sciences, China), Shumin Peng (Zhengzhou University, China), and Ya Li (University of Chinese Academy of Sciences, China)

TrustyShare: A Sharing Scheme using ARM TrustZone .1741
Yongkang Wu (Institute of Information Engineering), Langyue He (Institute of Information Engineering), Yiwei Shan (University of Chinese Academy of Sciences, China), Pengcheng Zhang (Institute of Information Engineering), Min He (Institute of Information Engineering), and Zhi Yang (Beijing Trusted Huatai Information Technology Co., Ltd)

SmartLED: Smartphone-Based Covert Channels Leveraging the Notification LED .1748
Lorena Gonzalez-Manzano (Universidad Carlos III de Madrid, Spain), Sergio Bernardez (Universidad Carlos III de Madrid, Spain), and Jose M. de Fuentes (Universidad Carlos III de Madrid, Spain)

Semantic Redirection Obfuscation: A Control flow Obfuscation Based on Android Runtime .1756.
Zhichao Wang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences), Yiwei Shan (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Zhi Yang (Beijing Trusted Huatai Information Technology Co., Ltd), Ruoyi Wang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences), and Shuang Song (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences)

Blockchain Based PKI and Certificates Management in Mobile Networks .1764.....
Junzhi Yan (China Mobile Research Institute, China), Xiaoyong Hang (China Mobile Research Institute, China), Bo Yang (China Mobile Research Institute, China), Li Su (China Mobile Research Institute, China), and Shen He (China Mobile Research Institute, China)

Monitoring Social Media for Vulnerability-Threat Prediction and Topic Analysis .1771.....
Shin-Ying Huang (Institute for Information Industry, Taiwan) and Tao Ban (National Institute of Information and Communications Technology, Japan)

Android Malware Classification Using Machine Learning and Bio-Inspired Optimisation Algorithms .1777.....
Jack Pye (Northmbria University, UK), Biju Issac (Northmbria University, UK), Nauman Aslam (Northmbria University, UK), and Husnain Rafiq (Northmbria University, UK)

LTMS: A Lightweight Trust Management System for Wireless Medical Sensor Networks .1783.....
Muhammad Shadi Hajar (Robert Gordon University, United Kingdom), M. Omar Al-Kadri (Robert Gordon University, United Kingdom), and Harsha Kalutarage (Robert Gordon University, United Kingdom)

Trust and Believe - Should We? Evaluating the Trustworthiness of Twitter Users .1791.....
Tanveer Khan (Network and Information Security Group, Tampere University, Finland) and Antonis Michalas (Network and Information Security Group, Tampere University, Finland)

Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things .1801.....
Theo Dimitrakos (German Research Center, Huawei Technologies Duesseldorf GmbH, Munich, Germany; University of Kent, Canterbury, UK), Tezcan Dilshener (German Research Center, Huawei Technologies Duesseldorf GmbH, Munich, Germany; European Business School University, Munich, Germany), Alexander Kravtsov (Israel Research Center, Huawei Technologies Co, Tel-Aviv, Israel), Antonio La Marra (Security Forge, Pisa, Italy), Fabio Martinelli (Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy), Athanasios Rizos (German Research Center, Huawei Technologies Duesseldorf GmbH, Munich, Germany), Alessandro Rosetti (Security Forge, Pisa, Italy), and Andrea Saracino (Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy)

pcSVF: An Evaluation of Side-Channel Vulnerability of Port Contention .1813
Xiaoyang Liu (University of Chinese Academy of Science, China) and Ziyuan Zhu (University of Chinese Academy of Science, China)

A Multi-layer Industrial-IoT Attack Taxonomy: Layers, Dimensions, Techniques and Application .1820
Syed Ghazanfar Abbas (University of Engineering and Technology, Lahore, Pakistan), Fabiha Hashmat (University of Engineering and Technology, Lahore, Pakistan), and Ghalib A. Shah (University of Engineering and Technology, Lahore, Pakistan)

A Semantic Model-Based Security Engineering Framework for Cyber-Physical Systems .1826
Andreas Aigner (Landshut University of Applied Science, Germany) and Abdelmajid Khelil (Landshut University of Applied Science, Germany)

Attribute-Based Data Access Control for Multi-authority System .1834
Ahmad Salehi S. (Monash University, Australia), Carsten Rudolph (Monash University, Australia), and Marthie Grobler (Distributed Systems Security, CSIRO's Data61, Australia)

DNRTI: A Large-Scale Dataset for Named Entity Recognition in Threat Intelligence .1842
Xuren Wang (Capital Normal University, China), Xinpei Liu (Capital Normal University, China), Shengqin Ao (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Ning Li (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhengwei Jiang (Institute of Information Engineering, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zongyi Xu (Capital Normal University, China), Zihan Xiong (Capital Normal University, China), Mengbo Xiong (Capital Normal University, China), and Xiaoqing Zhang (Capital Normal University, China)

AndroTIME: Identifying Timing Side Channels in the Android API .1849
Gerald Palfinger (A-SIT Secure Information Technology Center Austria, Austria), Bernd Prünster (Institute for Applied Information Processing and Communications, Graz University of Technology, Austria), and Dominik Julian Ziegler (Know-Center GmbH, Austria)

FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication .1857
Eric Klieme (University of Potsdam), Jonathan Wilke (University of Potsdam), Niklas van Dornick (University of Potsdam), and Christoph Meinel (University of Potsdam)

A Blockchain-Based Key Management Protocol for Secure Device-to-Device Communication in the Internet of Things .1868
Mohamed Ali Kandi (Sorbonne Université, Université de Technologie de Compiègne, CNRS, France), Djamel Eddine Kouicem (Sorbonne Université, Université de Technologie de Compiègne, CNRS, France), Hicham Lakhlef (Sorbonne Université, Université de Technologie de Compiègne, CNRS, France), Abdelmadjid Bouabdallah (Sorbonne Université, Université de Technologie de Compiègne, CNRS, France), and Yacine Challal (Laboratoire de Méthodes de Conception de Systèmes, École nationale Supérieure d'Informatique, Algiers, Algeria)

Finding Geometric Medians with Location Privacy .1874
Eyal Nussbaum (Ben Gurion University, Israel) and Michael Segal (Ben Gurion University, Israel)

Security and Privacy Analysis of Mhealth Application: A Case Study .1882
Wanrong Zhao (Kennesaw State University, United States), Hossain Shahriar (Kennesaw State University, United States), Victor Clincy (Kennesaw State University, United States), and Zakirul Alam Bhuiyan (Fordham University, United States)

Enabling Security Analysis of IoT Device-to-Cloud Traffic .1888
Eda Zhou (Worcester Polytechnic Institute, USA), Joseph Turcotte (Worcester Polytechnic Institute, USA), and Lorenzo De Carli (Worcester Polytechnic Institute, USA)

Towards A New Approach to Identify WhatsApp Messages .1895
Rick Cents (Politie Nederland, Utrecht, The Netherlands) and Nhien-An Le-Khac (University College Dublin, Ireland)

The 3rd International Workshop on Blockchain Systems and Applications (BlockchainSys 2020)

Session BlockchainSys-1

Efficient Off-Chain Transaction to Avoid Inaccessible Coins in Cryptocurrencies .1903
Hossein Rezaeighaleh (University of Central Florida, USA) and Cliff C. Zou (University of Central Florida, USA)

Assessing the Similarity of Smart Contracts by Clustering Their Interfaces .1910
Monika di Angelo (TU Wien, Austria) and Gernot Salzer (TU Wien, Austria)

Securing Manufacturing Using Blockchain .1920
Zahra Jadidi (Queensland University of Technology (QUT)), A. Dorri (Queensland University of Technology (QUT)), R. Jurdak (Queensland University of Technology (QUT)), and C. Fidge (Queensland University of Technology (QUT))

SCUR: Smart Contracts with a Static Upper-Bound on Resource Usage .1926
Markus Knecht (Communication Systems Group CSG, University of Zürich UZH, Switzerland; Institute for Mobile and Distributed Systems IMVS, University of Applied Sciences Northwestern Switzerland, Switzerland) and Burkhard Stiller (Communication Systems Group CSG, University of Zürich UZH, Switzerland)

SSIBAC: Self-Sovereign Identity Based Access Control .1935
Rafael Belchior (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal), Benedikt Putz (Chair of Information Systems, University of Regensburg, Germany), Guenther Pernul (Chair of Information Systems, University of Regensburg, Germany), Miguel Correia (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal), André Vasconcelos (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal), and Sérgio Guerreiro (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal)

A Privacy-Preserving Crowdsensing System with Muti-blockchain .1944
Tao Peng (Guangzhou University, Guangzhou, P. R. China), Jierong Liu (Guangzhou University, Guangzhou, P. R. China), Jianer Chen (Guangzhou University, Guangzhou, P. R. China), and Guojun Wang (Guangzhou University, Guangzhou, P. R. China)

A Blockchain-Based Vehicle-Trust Management Framework Under a Crowdsourcing Environment 1950
Dawei Wang (Jiangsu University, China), Xiao Chen (University of Edinburgh, UK), Haiqin Wu (University of Copenhagen, Denmark), Ruozhou Yu (North Carolina State University, USA), and Yishi Zhao (China University of Geosciences, China)

Permission Token Segmentation Scheme Based on Blockchain Access Control .1956
Jinshan Shi (Inner Mongolia University, China) and Ru Li (Inner Mongolia University, China)

A Blockchain-Based Pattern for Confidential and Pseudo-Anonymous Contract Enforcement .1965
Nicolas Six (Université Paris 1 Panthéon-Sorbonne, France), Claudia Negri Ribalta (Université Paris 1 Panthéon-Sorbonne, France), Nicolas Herbaut (Université Paris 1 Panthéon-Sorbonne, France), and Camille Salinesi (Université Paris 1 Panthéon-Sorbonne, France)

The 2020 International Workshop on Machine Learning for Trust, Security and Privacy in Computing and Communications (MLTrustCom 2020)

Session MLTrustCom-1

Detecting Online Game Malicious Chargeback by using k-NN .1971
Yu-Chih Wei (Information and Finance Management, National Taipei University of Technology), You-Xin Lai (Information and Finance Management, National Taipei University of Technology), Hai-Po Su (9Splay Entertainment Technology Co., LTD.), and Yu-Wen Yen (9Splay Entertainment Technology Co., LTD.)

A Novel Q-Learning Algorithm Based on the Stochastic Environment Path Planning Problem .1977
Jian Li (The Faculty of Computer Science and Engineering, Xi'an University of Technology, Shaanxi), Fei Rong (The Faculty of Computer Science and Engineering, Xi'an University of Technology, Shaanxi), and Yu Tang (The Faculty of Computer Science and Engineering, Xi'an University of Technology, Shaanxi)

Boosting Homograph Attack Classification Using Ensemble Learning and N-Gram Model .1983
Tran Phuong Thao (The University of Tokyo, Japan), Hoang-Quoc Nguyen-Son (KDDI Research, Inc., Japan), Rie Shigetomi Yamaguchi (The University of Tokyo, Japan), and Toshiyuki Nakata (The University of Tokyo, Japan)

Survey on Blockchain and Deep Learning .1989
Yizhuo Zhang (Fuzhou University, China), Yiwei Liu (Fuzhou University, China), and Chi-Hua Chen (Fuzhou University, China)

Special-Purpose Model Extraction Attacks: Stealing Coarse Model with Fewer Queries 1995
Rina Okada (NTT Secure Platform Laboratories, Japan), Zen Ishikura (NTT West Corp. Osaka, Japan), Toshiki Shibahara (NTT Secure Platform Laboratories, Japan), and Satoshi Hasegawa (NTT Secure Platform Laboratories, Japan)

The 2020 International Workshop on Smart Technologies for Intelligent Transportation and Communications (SmartITC 2020)

Session SmartITC-1

A Low-Cost Method for Accurate Localization of Traffic Participants 2001
Maozhu Liao (Intelligent Transportation, Institute of Software Chinese Academy of Sciences, China), Shengdong Chen (Intelligent Transportation, Institute of Software Chinese Academy of Sciences, China), Chuangjie Zheng (Intelligent Transportation, Institute of Software Chinese Academy of Sciences, China), and Feng Yuan (Institute of Software Chinese Academy of Sciences, China)

Integration of 5G, VANETs and Blockchain Technology 2007
Muhammad Arif (Guangzhou University, China), Walter Balzano (University of Naples, Italy), Alessandro Fontanella (University of Naples, Italy), Silvia Stranieri (University of Naples, Italy), Guojun Wang (Guangzhou University, China), and Xiaofei Xing (Guangzhou University, China)

Aquatic Drone Control Using Inertial Sensors - Comparative Filtering Methods 2014
Mihaela Hnatiuc (Constanta Maritime University, Romania), Oana Geman (Stefan cel Mare University, Romania), Dragos Vicoveanu (Stefan cel Mare University, Romania), and George Motru (Romanian Ait Traffic Services Adm, Romania)

Factors Affecting Trust in the Autonomous Vehicle: A Survey of Primary School Students and Parent Perceptions 2020
Yingying Ma (CAS Key Laboratory of Behavioral Science, Institute of Psychology, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Shuo Li (CAS Key Laboratory of Behavioral Science, Institute of Psychology, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China; Nankai University, China), Shaotian Qin (Renmin University of China, China), and Yue Qi (Renmin University of China, China; CAS Key Laboratory of Behavioral Science, Institute of Psychology, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

Prediction of Radio Frequency Spectrum Occupancy 2028
Hubert Kyeremateng-Boateng (Bowie State University, America), Marvin Conn (Computational and Information Sciences Directorate Army Research Laboratory, America), Darsana Josyula (Bowie State University, America), and Manohar Mareboyana (Bowie State University, America)

Author Index