

**2022 52nd Annual IEEE/IFIP
International Conference on
Dependable Systems and
Networks Workshops
(DSN-W 2022)**

**Baltimore, Maryland, USA
27 – 30 June 2022**



IEEE Catalog Number: CFP2241K-POD
ISBN: 978-1-6654-0263-7

**Copyright © 2022 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:	CFP2241K-POD
ISBN (Print-On-Demand):	978-1-6654-0263-7
ISBN (Online):	978-1-6654-0262-0
ISSN:	2325-6648

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

CURRAN ASSOCIATES INC.
proceedings
.com

2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN- W) **DSN-W 2022**

Table of Contents

Welcome from the DSN 2022 General Chairs	x
Message from the DSN 2022 Workshop Chairs	xi
Message from the SSIV 2022 Organizers	xiii
Message from the DSML 2022 Organizers	xiv
Message from the DCDS 2022 Organizers	xvi
Message from the AITS 2022 Organizers	xvii

8th Workshop on Safety and Security in Intelligent Vehicles (SSIV)

Stealthy Data Corruption Attack Against Road Traffic Congestion Avoidance Applications	1
<i>Aawista Chaudhry (Queen's University, Canada), Talal Halabi (University of Winnipeg, Canada), and Mohammad Zulkernine (Queen's University, Canada)</i>	
Certify the Uncertified: Towards Assessment of Virtualization for Mixed-Criticality in the Automotive Domain	8
<i>Marcello Cinque (Federico II di Napoli, Italy), Luigi De Simone (Federico II di Napoli, Italy), and Andrea Marchetta (Federico II di Napoli, Italy)</i>	
Tiny Black Boxes: A nano-Drone Safety Architecture	12
<i>Connor Sexton (California Polytechnic State University, San Luis Obispo) and Joseph Callenes (California Polytechnic State University, San Luis Obispo)</i>	
Alternative Route-Based Attacks in Metropolitan Traffic Systems	20
<i>Sidney La Fontaine (Northeastern University, USA), Naveen Muralidhar (Northeastern University, USA), Michael Clifford (Toyota InfoTech Labs, USA), Tina Eliassi-Rad (Northeastern University, USA), and Cristina Nita-Rotaru (Northeastern University, USA)</i>	

5th Workshop on Dependable and Secure Machine Learning (DSML)

Autonomous Attack Mitigation for Industrial Control Systems	28
<i>John Mern (Stanford University, USA), Kyle Hatch (Stanford University, USA), Ryan Silva (Johns Hopkins University Applied Physics Laboratory, USA), Cameron Hickert (Johns Hopkins University Applied Physics Laboratory, USA), Tamim Sookoor (Johns Hopkins University Applied Physics Laboratory, USA), and Mykel J. Kochenderfer (Stanford University, USA)</i>	
Federated Learning with Anomaly Client Detection and Decentralized Parameter Aggregation	37
<i>Shu Liu (Beijing University of Posts and Telecommunications, China) and Yanlei Shang (Beijing University of Posts and Telecommunications, China)</i>	
Robustness Testing of Data and Knowledge Driven Anomaly Detection in Cyber-Physical Systems	44
<i>Xugui Zhou (University of Virginia, USA), Maxfield Kouzel (University of Virginia, USA), and Homa Alemzadeh (University of Virginia, USA)</i>	
On the Impact of non-IID Data on the Performance and Fairness of Differentially Private Federated Learning	52
<i>Saba Amiri (University of Amsterdam, The Netherlands), Adam Belloum (University of Amsterdam, The Netherlands), Eric Nalisnick (University of Amsterdam, The Netherlands), Sander Klous (University of Amsterdam, The Netherlands), and Leon Gommans (Air France - KLM, The Netherlands)</i>	
A Robust Framework for Adaptive Selection of Filter Ensembles to Detect Adversarial Inputs.....	59
<i>Arunava Roy (The University of Memphis, USA) and Dipankar Dasgupta (The University of Memphis, USA)</i>	
Towards Building Resilient Ensembles Against Training Data Faults	68
<i>Abraham Chan (The University of British Columbia, Canada), Arpan Gujarati (The University of British Columbia, Canada), Karthik Pattabiraman (The University of British Columbia, Canada), and Sathish Gopalakrishnan (The University of British Columbia, Canada)</i>	
General Probability in Coq	70
<i>Avraham Shinnar (IBM Research) and Barry Trager (IBM Research)</i>	

4th Workshop on Data-Centric Dependability and Security (DCDS)

Data-Centric Analysis of Compound Threats to Critical Infrastructure Control Systems	72
<i>Sahiti Bommareddy (Johns Hopkins University, USA), Benjamin Gilby (University of Pittsburgh, USA), Maher Khan (University of Pittsburgh, USA), Imes Chiu (U.S. Army Corps of Engineers (USACE), USA), Mathaios Panteli (University of Cyprus, Greece), John W. van de Lindt (Colorado State University, USA), Linton Wells II (Center for Resilient and Sustainable Communities (C-RASC), George Mason University, USA), Yair Amir (Johns Hopkins University, USA), and Amy Babay (University of Pittsburgh, USA)</i>	
Network Message Field Type Clustering for Reverse Engineering of Unknown Binary Protocols	80
<i>Stephan Kleber (Ulm University, Germany), Frank Kargl (Ulm University, Germany), Milan Stute (Technical University of Darmstadt, Germany), and Matthias Hollick (Technical University of Darmstadt, Germany)</i>	

A Dataset of Linux Failure Data for Dependability Evaluation and Improvement	88
<i>João R. Campos (University of Coimbra, Portugal), Ernesto Costa (University of Coimbra, Portugal), and Marco Vieira (University of Coimbra, Portugal)</i>	
Privacy Leakage Analysis for Colluding Smart Apps	96
<i>Junzhe Wang (University of South Carolina, USA) and Lannan Luo (University of South Carolina, USA)</i>	
A Practical Security Evaluation of a Moving Target Defence Against Multi-Phase Cyberattacks	103
<i>Tina Moghaddam (University of Queensland, Australia), Minjune Kim (University of Queensland, Australia), Jin-Hee Cho (Virginia Tech, USA), Hyuk Lim (Korea Institute of Energy Technology (KENTECH), Republic of Korea), Terrence J. Moore (US Army Research Lab., USA), Frederica F. Nelson (US Army Research Lab., USA), and Dan Dongseong Kim (University of Queensland, Australia)</i>	

2nd Workshop on Artificial Intelligence To Security (AITS)

Repairing Security Vulnerabilities Using Pre-Trained Programming Language Models	111
<i>Kai Huang (Xidian University, China; University of Chinese Academy of Sciences, China), Su Yang (University of Chinese Academy of Sciences, China), Hongyu Sun (Xidian University, China; University of Chinese Academy of Sciences, China), Chengyi Sun (University of Chinese Academy of Sciences, China), Xuejun Li (Xidian University, China), and Yuqing Zhang (Xidian University, China; University of Chinese Academy of Sciences, China; Hainan University, China)</i>	
An Overview of Sybil Attack Detection Mechanisms in VFC	117
<i>Haonan Yang (Hainan University, China; University of Chinese Academy of Sciences, China), Yongchao Zhong (Hainan University, China; University of Chinese Academy of Sciences, China), Bo Yang (Hainan University, China; University of Chinese Academy of Sciences, China), Yiyu Yang (University of Chinese Academy of Sciences, China), Zifeng Xu (Hainan University, China), Longjuan Wang (Hainan University, China), and Yuqing Zhang (Hainan University, China; University of Chinese Academy of Sciences, China)</i>	
A Chinese Multi-modal Relation Extraction Model for Internet Security of Finance	123
<i>Qinghan Lai (Qilu University of Technology (Shandong Academy of Sciences), China), Shuai Ding (Qilu University of Technology (Shandong Academy of Sciences), China), Jinghao Gong (Qilu University of Technology (Shandong Academy of Sciences), China), Jin'an Cui (Qilu University of Technology (Shandong Academy of Sciences), China), and Song Liu (Qilu University of Technology (Shandong Academy of Sciences), China)</i>	

SbrPBert: A BERT-Based Model for Accurate Security Bug Report Prediction	129
<i>Xudong Cao (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China), Tianwei Liu (School of Cyber Engineering, Xidian University, China), Jiayuan Zhang (School of Computer and Communication, Lanzhou University of Technology, China), Mengyue Feng (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China), Xin Zhang (School of Cyberspace Security, Xi'an University of Posts and Telecommunications, China), Wanying Cao (National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China), Hongyu Sun (School of Cyber Engineering, Xidian University, China), and Yuqing Zhang (University of Chinese Academy of Sciences, China)</i>	
SCUC-DSAC: A Data Sharing Access Control Model Based on Smart Contract and User Credit	135
<i>Guangxia Xu (Chongqing University of Posts and Telecommunications, China) and Li Wang (Chongqing University of Posts and Telecommunications, China)</i>	
Vulnerability Dataset Construction Methods Applied to Vulnerability Detection: A Survey	141
<i>Yuhao Lin (Hainan University, China; University of Academy of Sciences, China), Ying Li (Hainan University, China; University of Academy of Sciences, China), Mianxue Gu (Hainan University, China; University of Academy of Sciences, China), Hongyu Sun (Xidian University, China; Hainan University, China), Qiuling Yue (Hainan University, China), Jinglu Hu (Waseda University, Japan), Chunjie Cao (Hainan University, China), and Yuqing Zhang (Hainan University, China; University of Chinese Academy of Sciences, China; Xidian University, China)</i>	
Multi-Authoritative Users Assured Data Deletion Scheme in Cloud Computing	147
<i>Junfeng Tian (School of Cyberspace Security and Computer Institute Hebei University, China), Ruxin Bai (School of Cyberspace Security and Computer Institute Hebei University, China), and Tianfeng Zhang (School of Cyberspace Security and Computer Institute Hebei University, China)</i>	
A Two-Layer Soft-Voting Ensemble Learning Model for Network Intrusion Detection	155
<i>Wenbin Yao (Beijing University of Posts and Telecommunications, China), Yingying Hou (Beijing University of Posts and Telecommunications, China), Longcan Hu (Beijing University of Posts and Telecommunications, China), and Xiaoyong Li (Beijing University of Posts and Telecommunications, China)</i>	
Machine Learning Analysis of Memory Images for Process Characterization and Malware Detection	162
<i>Seth Lyles (Lawrence Livermore National Lab), Kristine Monteith (Lawrence Livermore National Lab), Micaela Gallegos (Lawrence Livermore National Lab), John Donaldson (Lawrence Livermore National Lab), Claire Taylor (Lawrence Livermore National Lab), and Hannah Nyholm (Lawrence Livermore National Lab)</i>	
Blockchain-Based Incentive and Arbitrable Data Auditing Scheme	170
<i>Junfeng Tian (Computer Institute Hebei University, China), Qianqian Song (Computer Institute Hebei University, China), and Haoning Wang (Computer Institute Hebei University, China)</i>	

A Comprehensive Dynamic Quality Assessment Method for Cyber Threat Intelligence	178
<i>Menghan Wang (Northwestern Polytechnical University, China), Libin Yang (Northwestern Polytechnical University, China), and Wei Lou (The Hong Kong Polytechnic University, China)</i>	
DTC: A Dynamic Trusted Collaboration Architecture for Mobile Edge Computing	182
<i>Ruizhong Du (Hebei University, China) and Yan Gao (Hebei University, China)</i>	
VDBWGD: Vulnerability Detection Based on Weight Graph and Deep Learning	186
<i>Xin Zhang (Xi'an University of Posts and Telecommunications, China; University of Chinese Academy of Sciences, China), Hongyu Sun (Xidian University, China; University of Chinese Academy of Sciences, China), Zhipeng He (Xi'an University of Posts and Telecommunications, China; University of Chinese Academy of Sciences, China), Mianxue Gu (Hainan University, China; University of Chinese Academy of Sciences, China), Jingyu Feng (Xi'an University of Posts and Telecommunications, China), and Yuqing Zhang (Xi'an University of Posts and Telecommunications, China; University of Chinese Academy of Sciences, China; Xidian University, China; Hainan University, China)</i>	
Dynamic Multipath Routing Mechanism for Multimedia Data Flow Scheduling Over Software Defined Networks	191
<i>Wu Jiawei (College of Information Engineering, China Jiliang University, P. R. China), Qiao Xiuquan (State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China), Lu Huijuan (College of Information Engineering, China Jiliang University, P. R. China), and Junliang Chen (State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China)</i>	
Author Index	199