

**2024 54th Annual IEEE/IFIP  
International Conference on  
Dependable Systems and  
Networks Workshops  
(DSN-W 2024)**

**Brisbane, Australia  
24-27 June 2024**



**IEEE Catalog Number: CFP2441K-POD  
ISBN: 979-8-3503-9573-0**

**Copyright © 2024 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:	CFP2441K-POD
ISBN (Print-On-Demand):	979-8-3503-9573-0
ISBN (Online):	979-8-3503-9572-3
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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN- W) **DSN-W 2024**

## Table of Contents

Message from the General Chairs .....	viii
Message from the Workshop Chairs .....	x
Message from the DCCS Workshop Chairs .....	xii
Message from the DSML Workshop Chairs .....	xiii
Message from the VERDI Workshop Chairs .....	xiv
Organization (DCCS) .....	xv
Organization (DSML) .....	xvi
Organization (VERDI) .....	xvii
Keynote (DCCS) .....	xviii
Keynote (DSML) .....	xx
Keynote (VERDI) .....	xxii

### DCCS24 Workshop

DDoShield-IoT: A Testbed for Simulating and Lightweight Detection of IoT Botnet DDoS Attacks .....	1
<i>Simona De Vivo (University of Naples Federico II, Italy), Islam Obaidat (University of North Carolina at Charlotte, USA), Dong Dai (University of North Carolina at Charlotte, USA), and Pietro Liguori (University of Naples Federico II, Italy)</i>	
Performance Comparison of Bayesian Estimations on the Residual Number of Software Bugs .....	9
<i>Yuki Hagiwara (Hiroshima University, Japan), Tadashi Dohi (Hiroshima University, Japan), and Hiroyuki Okamura (Hiroshima University, Japan)</i>	
Caching and Prefetching for Improving ORAM Performance .....	17
<i>Naohiro Hayashibara (Kyoto Sangyo University, Japan) and Kazuaki Kawabata (Kyoto Sangyo University, Japan)</i>	
On Predicting Software Intensity Using Wavelets and Nonlinear Regression .....	21
<i>Kaoru Matsui (Tokyo Metropolitan University, Japan) and Xiao Xiao (Tokyo Metropolitan University, Japan)</i>	

## DSML24 Workshop

Measuring the Effects of Environmental Influences on Object Detection .....	29
<i>Niklas Bunzel (Fraunhofer SIT/ATHENE/TU-Darmstadt, Germany), Michel Geißler (TU-Darmstadt, Germany), and Gerrit Klause (Fraunhofer SIT/ATHENE, Germany)</i>	
Intrusion Detection Systems Using Quantum-Inspired Density Matrix Encodings .....	32
<i>Larry Huynh (University of Western Australia, Australia), Jin B. Hong (University of Western Australia, Australia), Ajmal Mian (University of Western Australia, Australia), Hajime Suzuki (Commonwealth Scientific and Industrial Research Organisation (CSIRO)'s Data61, Australia), and Seyit Camtepe (Commonwealth Scientific and Industrial Research Organisation (CSIRO)'s Data61, Australia)</i>	
Adversarial Patch Detection: Leveraging Depth Contrast for Enhanced Threat Visibility .....	39
<i>Niklas Bunzel (Fraunhofer SIT/ATHENE/TU-Darmstadt, Germany) and Jannis Hamburg (Hochschule Darmstadt/ATHENE, Germany)</i>	
Unlearning Backdoor Attacks Through Gradient-Based Model Pruning .....	46
<i>Kealan Dunnett (Queensland University of Technology; CSIRO's Data61), Reza Arablouei (CSIRO's Data61), Dimity Miller (Queensland University of Technology), Volkan Dedeoglu (Queensland University of Technology; CSIRO's Data61), and Raja Jurdak (Queensland University of Technology)</i>	
TrustDDL: A Privacy-Preserving Byzantine-Robust Distributed Deep Learning Framework .....	55
<i>René Klaus Nikiel (TU Darmstadt, Germany), Meghdad Mirabi (DFKI &amp; TU Darmstadt, Germany), and Carsten Binnig (TU Darmstadt &amp; DFKI, Germany)</i>	
Hybrid Convolutional Neural Networks with Reliability Guarantee .....	63
<i>Hans Dermot Doran (Zurich University of Applied Sciences, Switzerland) and Suzana Veljanovska (Zurich University of Applied Sciences, Switzerland)</i>	
Universal Soldier: Using Universal Adversarial Perturbations for Detecting Backdoor Attacks .....	66
<i>Xiaoyun Xu (Radboud University Nijmegen, The Netherlands), Oguzhan Ersoy (Radboud University Nijmegen, The Netherlands), Behrad Tajalli (Radboud University Nijmegen, The Netherlands), and Stjepan Picek (Radboud University Nijmegen, The Netherlands)</i>	

## VERDI Workshop

Highly Comprehensive and Efficient Memory Safety Enforcement with Pointer Tagging .....	74
<i>Xiaolei Wang (National University of Defense Technology, China), Bin Zhang (National University of Defense Technology, China), Chaojing Tang (National University of Defense Technology, China), and Long Zhang (Institute of Systems Engineering, AMS, China)</i>	
Enhancing Continuous Risk Assessment: The Role of Safety Engineers in Early Hazard Identification .....	82
<i>Anil Ranjithbhai Patel (RPTU Kaiserslautern-Landau, Germany) and Peter Liggesmeyer (Fraunhofer IESE, Germany)</i>	

Virtual Evaluation of Dependability Attributes for Mission-Critical Cyber-Physical Systems .....	90
<i>Adam Bachorek (Fraunhofer IESE, Germany), Benedikt Lüken-Winkels (Fraunhofer IESE, Germany), Iron Prando da Silva (Fraunhofer IESE, Germany), Stefan Schwenk (Fraunhofer IESE, Germany), Markus Damm (Fraunhofer IESE, Germany), and Pablo Oliveira Antonino (Fraunhofer IESE, Germany)</i>	
Hybrid Hardware/Software Detection of Multi-Bit Upsets in Memory .....	94
<i>Robin Thunig (TU Dresden, Germany), Christoph Borchert (Osnabrück University, Germany), Urs Kober (TU Dresden, Germany), and Horst Schirmeier (TU Dresden, Germany)</i>	
Cybersecurity Pathways Towards CE-Certified Autonomous Forestry Machines .....	98
<i>Mazen Mohamad (RISE Research Institutes of Sweden, Sweden), Ramana Reddy Avula (RISE Research Institutes of Sweden, Sweden), Peter Folkesson (RISE Research Institutes of Sweden, Sweden), Pierre Kleberger (RISE Research Institutes of Sweden, Sweden), Aria Mirzai (RISE Research Institutes of Sweden, Sweden), Martin Skoglund (RISE Research Institutes of Sweden, Sweden), and Marvoin Damschen (RISE Research Institutes of Sweden, Sweden)</i>	
<b>Author Index .....</b>	<b>107</b>