

2023 IEEE Conference on Dependable and Secure Computing (DSC 2023)

**Tampa, Florida, USA
7-9 November 2023**



**IEEE Catalog Number: CFP23J65-POD
ISBN: 979-8-3503-8212-9**

**Copyright © 2023 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:	CFP23J65-POD
ISBN (Print-On-Demand):	979-8-3503-8212-9
ISBN (Online):	978-8-3503-8211-2

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

Table of Contents

An Observer-Based Control for a Networked Control of Permanent Magnet Linear Motors under a False-Data-Injection Attack	1
<i>Parisa Ansari Bonab, James Holland and Arman Sargolzaei</i>	
Impact of Topology Noise on Power Systems State Estimation Using a Temporal GCN Framework	9
<i>Seyed Hamed Haghshenas and Mia Naeini</i>	
Designing and Testing A Secure Cooperative Adaptive Cruise Control under False Data Injection Attack	14
<i>Jonas Cunningham-Rush, James Holland, Shirin Noei and Arman Sargolzaei</i>	
RIDE: Real-time Intrusion Detection via Explainable Machine Learning Implemented in a Memristor Hardware Architecture	22
<i>Jingdi Chen, Lei Zhang, Joseph Riem, Gina Adam, Nathaniel D. Bastian and Tian Lan</i>	
CoDex: Cross-Tactic Correlation System for Data Exfiltration Detection	30
<i>Shanhsin Lee, Yung-Shiu Chen and Shihpyng Shieh</i>	
Secure Outsourcing of Boolean Formulas Truth Assignment Problem	38
<i>Albert Guan</i>	
Decentralized and Incentivized Voting System with Web3 Technology Ensuring Anonymity and Preventing Double Voting	43
<i>Lo-Yao Yeh, Jun-Qian Jian and Jen-Wei Hu</i>	
Cyber Risk Evaluation for Android-based Devices	51
<i>Ocheme Anthony Ekle and Denis Ulybyshev</i>	
Lightweight Digital Signatures for Internet of Things: Current and Post-Quantum Trends and Visions	59
<i>Saif Eddine Nouma and Attila Altay Yavuz</i>	
Detecting Web Application DAST Attacks with Machine Learning	61
<i>Pojan Shahrivar, Stuart Millar and Ezzeldin Shereen</i>	
APTer: Towards the Investigation of APT Attribution	69
<i>Vinay Sachidananda, Rajendra Patil, Akshay Sachdeva, Kwok-Yan Lam and Yang Liu</i>	
A Study on the Forensic Analysis of Airlines Applications on Android Operating System .	79
<i>Urva Maryam and Mehdi Hussain</i>	
SRAM and Generative Network-based Physical Fingerprinting for Trust Management in the Internet of Things	88
<i>Varun Kohli, Muhammad Naveed Aman and Biplab Sikdar</i>	
Privacy-Preserving Video Understanding via Transformer-based Federated Learning	96
<i>Keval Doshi and Yasin Yilmaz</i>	
Empirical Evaluation of Autoencoder Models for Anomaly Detection in Packet-based NIDS	104
<i>Soumyadeep Hore, Quoc Nguyen, Yulun Xu, Ankit Shah, Nathaniel Bastian and Trung Le</i>	

Highly optimized Curve448 and Ed448 design in wolfSSL and side-channel evaluation on Cortex-M4	112
<i>Mila Anastasova, Rabih El Khatib, Aimee Laclaustra, Reza Azarderakhsh and Mehran Mozaffari Kermani</i>	
Preprocessing Network Traffic using Topological Data Analysis for Data Poisoning Detection	120
<i>Galamo Monkam, Michael De Lucia and Nathaniel Bastian</i>	
Compiler-Supported Selective Software Fault Tolerance.....	128
<i>Tuncer Turhan, Hakan Tekgöl and Ozcan Ozturk</i>	
The Substitution-Boxes Incompatibility in JPEG Image Encryption	134
<i>Manuel Alejandro Cardona-López, Juan Carlos Chimal-Eguía, Víctor Manuel Silva-García and Rolando Flores-Carapia</i>	
Cyber Security in Blockchain.....	141
<i>Eric Cooper, Eric Weese, Alex Fortson, Dan Lo and Yong Shi</i>	
Semantic Video Transformer for Robust Action Recognition	152
<i>Keval Doshi and Yasin Yilmaz</i>	
Detection of Ransomware Attack Using Deep Learning	157
<i>Muna Jemal and Dan Lo</i>	
Privacy-Preserving and Fault-Tolerant Data Aggregation Protocol for Internet of Drones .	166
<i>Cong Pu</i>	
Enriching the Semantics of Information Flow Tracking with Source-Level Memory Allocation Event Logging	174
<i>Sanoop Mallisery and Yu-Sung Wu</i>	
SepMM : A General Matrix Multiplication Optimization Approach for Privacy-Preserving Machine Learning	184
<i>Tung-Lin Tsai and Pei-Yuan Wu</i>	
Data Provenance for IoT Devices by Exploiting Clock Variations	194
<i>Mirza Athar Baig and Muhammad Naveed Aman</i>	
AI Techniques for Software Vulnerability Detection and Mitigation	201
<i>Heba Khater, Mohamad Khayat, Saed Alrabae, Mohamed Adel Serhani, Ezedin Barka and Farag Sallabi</i>	
Towards Robust Learning using Diametrical Risk Minimization for Network Intrusion Detection	211
<i>Kelson McCollum, Nathaniel Bastian and Johannes Royset</i>	
FLID: Intrusion Attack and Defense Mechanism for Federated Learning-Empowered Connected Autonomous Vehicles	219
<i>Md Zarif Hossain, Ahmed Imteaj, Saika Zaman, Abdur R. Shahid, Sajedul Talukder and M. Hadi Amini</i>	
Automatic Conversion of ABAC Policies for RBAC Systems.....	227
<i>Maryam Davari and Mohammad Zulkernine</i>	

ML based Detection and Mitigation Scheme for DoS attacks on SDN Controllers	234
<i>Tamer Omar, Barret Griffin and Jose Garcia</i>	
Malicious Cyber Activity Detection using Zigzag Persistence	240
<i>Audun Myers, Alyson Bittner, Sinan Aksoy, Dan Best, Gregory Henselman-Petrusek, Helen Jenne, Cliff Joslyn, Bill Kay, Garret Seppala, Stephen Young and Emilie Purvine</i>	