

2023 Silicon Valley Cybersecurity Conference (SVCC 2023)

**San Jose, California, USA
17-19 May 2023**



**IEEE Catalog Number: CFP23DI5-POD
ISBN: 979-8-3503-2158-6**

**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:	CFP23DI5-POD
ISBN (Print-On-Demand):	979-8-3503-2158-6
ISBN (Online):	979-8-3503-2157-9

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

Trustworthy of Implantable Medical Devices Using ECG Biometric	1
<i>Nima Karimian, Sara Tehranipoor, Thomas Lyp</i>	
Lightweight and Effective Website Fingerprinting Over Encrypted DNS.....	7
<i>Yong Shao, Kenneth Hernandez, Kia Yang, Eric Chan-Tin, Mohammed Abuhamad</i>	
EGO-6: Enhancing Geofencing Security Systems with Optimal Deployment of 6G TRPs.....	15
<i>Alireza Famili, Angelos Stavrou, Haining Wang, Jung-Min Jerry Park</i>	
Anomaly Detection in Embedded Devices Through Hardware Introspection.....	23
<i>David Llanio Reyes, Alexander Perez-Pons, Rogelio Bofill Dean</i>	
WebTracker: Real Web browsing Behaviors	30
<i>Daisy Reyes, Eno Dynowski, Taryn Chovan, John Mikos, Eric Chan-Tin, Mohammed Abuhamad, Shelia Kennison</i>	
Multivariate Time Series Anomaly Detection with Deep Learning Models Leveraging Inter-Variable Relationships	38
<i>Changmin Seong, Dongjun Lim, Jiho Jang, Jonghoon Lee, Jong-Geun Park, Yun-Gyung Cheong</i>	
BlockNIC: SmartNIC Assisted Blockchain.....	46
<i>Eish Kapoor, Gavin Jampani, Sean Choi</i>	
Autonomous Lending Organization on Ethereum with Credit Scoring.....	54
<i>Thomas H. Austin, Katerina Potika, Chris Pollett</i>	
Guard Cache: Creating False Cache Hits and Misses to Mitigate Side-Channel Attacks.....	62
<i>Fernando Mosquera, Krishna Kavi, Gayatri Mehta, Lizy K. John</i>	
Malware Detection Through Contextualized Vector Embeddings.....	70
<i>Vinay Pandya, Fabio Di Troia</i>	
OFMCDM/IRF: A Phishing Website Detection Model Based on Optimized Fuzzy Multi-Criteria Decision-Making and Improved Random Forest.....	77
<i>Md Abdullah Al Ahasan, Mengjun Hu, Nashid Shahriar</i>	
A Curriculum Framework for Autonomous Network Defense Using Multi-Agent Reinforcement Learning	85
<i>Robert G. Campbell, Magdalini Eirinaki, Younghee Park</i>	
HoneyContainer: Container-Based Webshell Command Injection Defending and Backtracking	93
<i>Kuan-Chien Wang, Wei-Jun Cheng, Jie Zhang, Min-Te Sun, Kazuya Sakai, Wei-Shinn Ku</i>	
Privacy-Preserving Trust Management for Vehicular Communications and Federated Learning	101
<i>Sanghyun Byunx, Arijet Sarker, Ken Lew, Jugal Kalita, Sang-Yoon Chang</i>	
Investigation and Countermeasure Toward Unintentional Access to Docker Container	109
<i>Yueyang Li, Luyi Li, Ruxue Luo, Yuzhen Chen, Arijet Sarker, Sang-Yoon Chang, Wenjun Fan</i>	

Author Index