

2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA 2019)

**Los Angeles, California, USA
12 – 14 December 2019**



**IEEE Catalog Number: CFP19V08-POD
ISBN: 978-1-7281-6742-8**

**Copyright © 2019 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:	CFP19V08-POD
ISBN (Print-On-Demand):	978-1-7281-6742-8
ISBN (Online):	978-1-7281-6741-1

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

2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS- ISA) **TPS-ISA 2019**

Table of Contents

Message from the General Chairs and PC Chairs	ix
Organizing Committee	xi
Technical Program Committee	xii
Steering Committee	xiii
Keynote	xiv

Session 1: Trust, Security, and Privacy of Machine Learning

Safety and Consistency of Mutable Attributes Using Quotas: A Formal Analysis	1
<i>Mehrnoosh Shakarami (University of Texas at San Antonio) and Ravi Sandhu (University of Texas at San Antonio)</i>	
Z Table: Cost-Optimized Attack on Reinforcement Learning	10
<i>Ian Y. Garrett (Virginia Tech) and Ryan M. Gerdes (Virginia Tech)</i>	
Diggi: A Secure Framework for Hosting Native Cloud Functions with Minimal Trust	18
<i>Anders Tungeland Gjerdrum (UiT: The Arctic University of Norway), Håvard Dagenborg Johansen (UiT: The Arctic University of Norway), Lars Brenna (UiT: The Arctic University of Norway), and Dag Johansen (UiT: The Arctic University of Norway)</i>	
An Intelligent Behavior-Based Ransomware Detection System For Android Platform	28
<i>Abdulrahman Alzahrani (Oakland University), Hani Alshahrani (Najran University), Ali Alshehri (Oakland University), and Huirong Fu (Oakland University)</i>	

Session 2: Security and Privacy for Edge AI and IoT

Disincentivizing Double Spend Attacks Across Interoperable Blockchains	36
<i>Kuheli Sai (University of Pittsburgh) and David Tipper (University of Pittsburgh)</i>	

Design and Implementation of Privacy-Preserving, Flexible and Scalable Role-Based Hierarchical Access Control	46
<i>Tyler Phillips (Purdue University), Xiaoyuan Yu (Purdue University), Brandon Haakenson (Purdue University), and Xukai Zou (Purdue University)</i>	
ComplexIoT: Behavior-Based Trust For IoT Networks	56
<i>Kyle Haefner (Colorado State University) and Indrakshi Ray (Colorado State University)</i>	
An RNS Implementation of the Elliptic Curve Cryptography for IoT Security	66
<i>Jai Gopal Pandey (CSIR-Central Electronics Engineering Research Institute), Chhavi Mitharwal (CSIR-Central Electronics Engineering Research Institute), and Abhijit Karmakar (CSIR-Central Electronics Engineering Research Institute)</i>	

Session 3: Security and Privacy in Machine Learning

Machine Learning and Recognition of User Tasks for Malware Detection	73
<i>Yasamin Alagrash (Oakland University), Nithasha Mohan (Oakland University), Sandhya Rani Gollapalli (Oakland University), and Julian Rrushi (Oakland University)</i>	
Effects of Differential Privacy and Data Skewness on Membership Inference Vulnerability	82
<i>Stacey Truex (Georgia Institute of Technology), Ling Liu (Georgia Institute of Technology), Mehmet Emre Gursoy (Georgia Institute of Technology), Wenqi Wei (Georgia Institute of Technology), and Lei Yu (IBM Research)</i>	
Towards Deep Federated Defenses Against Malware in Cloud Ecosystems	92
<i>Joshua Payne (Stanford University) and Ashish Kundu (Nuro.ai)</i>	
Twitter Bot Detection Using Bidirectional Long Short-Term Memory Neural Networks and Word Embeddings	101
<i>Feng Wei (York University) and Uyen Trang Nguyen (York University)</i>	

Session 4: Security and Privacy by Design

Countering Malware Via Decoy Processes with Improved Resource Utilization Consistency	110
<i>Sara Sutton (Oakland University), Benjamin Bond (Oakland University), Sementa Tahiri (Oakland University), and Julian Rrushi (Oakland University)</i>	
Analysis and Nudging of Personally Identifiable Information in Online Used Markets	120
<i>Hyunsu Mun (Chungnam National University) and Youngseok Lee (Chungnam National University)</i>	
SERS: A Security-Related and Evidence-Based Ranking Scheme for Mobile Apps	130
<i>Nahida Sultana Chowdhury (Purdue University) and Rajeev R. Raje (Purdue University)</i>	
A Performance Evaluation of CAN Encryption	140
<i>Hanlin Chen (Purdue University) and Baijian Yang (Purdue University)</i>	

Session 5: Secure and Trusted Cyber-Space

Redistricting using Blockchain Network	150
<i>Naresh Adhikari (Mississippi State University), Naila Bushra (Mississippi State University), and Mahalingam Ramkumar (Mississippi State University)</i>	
Secure Queryable Dynamic Graphs using Blockchain	160
<i>Naila Bushra (Mississippi State University), Naresh Adhikari (Mississippi State University), and Mahalingam Ramkumar (Mississippi State University)</i>	
Data Siphoning Across Borders: The Role of Internet Tracking	168
<i>Ashwini Rao (Technical University of Munich) and Juergen Pfeffer (Technical University of Munich)</i>	
Open-TEE is No Longer Virtual: Towards Software-Only Trusted Execution Environments Using White-Box Cryptography	177
<i>Kemal Bicakci (TOBB University of Economics and Technology), Ihsan Kagan Ak (TOBB University of Economics and Technology), Betul Askin Ozdemir (Middle East Technical University), and Mesut Gozutok (Havelsan Inc.)</i>	

Session 6: Security and Privacy by Design

Factoring RSA Keys in the IoT Era	184
<i>Jonathan Kilgallin (Keyfactor) and Ross Vasko (Keyfactor)</i>	
Contextualizing Consensus Protocols in Blockchain: A Short Survey	190
<i>Golam Bashir (Boise State University), Graham Hill (Boise State University), Subroto Singha (Boise State University), Praneeth Marella (Boise State University), Gaby G. Dagher (Boise State University), and Jidong Xiao (Boise State University)</i>	
Towards Applying Design-Thinking for Designing Privacy-Protecting Information Systems	196
<i>Mortaza S. Bargh (The Hague, Rotterdam University of Applied Sciences) and Sunil Choenni (The Hague, Rotterdam University of Applied Sciences)</i>	
User Acceptance of Usable Blockchain-Based Research Data Sharing System: An Extended TAM-Based Study.....	203
<i>Ajay Kumar Shrestha (University of Saskatchewan) and Julita Vassileva (University of Saskatchewan)</i>	

Vision Track: Trust, Privacy, and Security in Intelligent Systems

Central Attribute Authority (CAA): A Vision for Seamless Sharing of Organizational Resources	209
<i>Saptarshi Das (Indian Institute of Technology Kharagpur), Shamik Sural (Indian Institute of Technology Kharagpur), Jaideep Vaidya (Rutgers University), and Vijayalakshmi Atluri (Rutgers University)</i>	

Securing Big Data in the Age of AI	218
<i>Murat Kantarcioglu (University of Texas at Dallas, Data Security Technologies LLC) and Fahad Shaon (University of Texas at Dallas, Data Security Technologies LLC)</i>	
Malware Containment in Cloud	221
<i>Abhishek Malvankar (IBM Thomas J. Watson Research Center), Joshua Payne (Stanford University), Karan K. Budhraj (University of Maryland), Ashish Kundu (IBM Thomas J. Watson Research Center), Suresh Chari (IBM Thomas J. Watson Research Center), and Mukesh Mohania (IIIT Delhi)</i>	
Secure Real-Time Heterogeneous IoT Data Management System	228
<i>Md Shihabul Islam (The University of Texas at Dallas), Harsh Verma (The University of Texas at Dallas), Latifur Khan (The University of Texas at Dallas), and Murat Kantarcioglu (The University of Texas at Dallas)</i>	
Robust (Deep) Learning Framework Against Dirty Labels and Beyond	236
<i>Amirmasoud Ghiassi (TU Delft), Taraneh Younesian (TU Delft), Zhilong Zhao (University of Grenoble), Robert Birke (ABB Future Labs), Valerio Schiavoni (University of Neuchatel), and Lydia Y. Chen (TU Delft)</i>	
Trustworthy Misinformation Mitigation with Soft Information Nudging	245
<i>Benjamin D. Horne (Rensselaer Polytechnic Institute), Mauricio Gruppi (Rensselaer Polytechnic Institute), and Sibel Adali (Rensselaer Polytechnic Institute)</i>	
Computer Systems Have 99 Problems, Let's Not Make Machine Learning Another One	255
<i>David Mohaisen (University of Central Florida) and Songqing Chen (George Mason University)</i>	
Next Generation Smart Built Environments: The Fusion of Empathy, Privacy and Ethics	260
<i>Denis Graanin (Virginia Tech), Ramoni O. Lasisi (Virginia Military Institute), Mohamed Azab (Virginia Military Institute), and Mohamed Eltoweissy (Virginia Military Institute)</i>	
Author Index	269