2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA 2021)

Virtual Conference
13 – 15 December 2021

IEEE Catalog Number: CFP21V08-POD
ISBN: 978-1-6654-1624-5

**Copyright © 2021 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:	CFP21V08-POD
ISBN (Print-On-Demand):	978-1-6654-1624-5
ISBN (Online):	978-1-6654-1623-8

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

2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)

TPS-ISA 2021

Table of Contents

Message from the General Chairs and PC Chairs xi
Organizing Committee xiii
Technical Program Committee xiv
Steering Committee xv
Keynotes xvi
Conference Panels xviii
Conference Tutorial xxv

Research Session 1

Hydra: Pipelineable Interactive Arguments of Knowledge for Verifiable Neural Networks 1
William Zhang (Ward Melville High School) and Yu Xia (MIT CSAIL)

Membership Inference Attack on Graph Neural Networks 11
Iyiola E. Olatunji (L3S Research Center, Germany), Wolfgang Nejdl (L3S Research Center, Germany), and Megha Khosla (L3S Research Center, Germany)

Towards Faster Functional Encryption for Privacy-Preserving Machine Learning 21
Prajwal Panzade (Georgia State University, USA) and Daniel Takabi (Georgia State University, USA)

Resilient and Verifiable Federated Learning Against Byzantine Colluding Attacks 31
Georges Kamhoua (Old Dominion University, USA), Eranga Bandara (Old Dominion University, USA), Peter Foytik (Old Dominion University, USA), Priyanka Aggarwal (Old Dominion University, USA), and Sachin Shetty (Old Dominion University, USA)

Research Session 2

Feature Reduction Through Data Preprocessing for Intrusion Detection in IoT Networks 41
Tania Tahmina Jui (Bangladesh University of Engineering and Technology, Bangladesh), Md. Nazmul Hoq (Concordia University, Canada), Suryadipta Majumdar (Concordia University, Canada), and Md. Shohrab Hossain (Bangladesh University of Engineering and Technology, Bangladesh)

Fides: Distributed Cyber-Physical Contracts 51
Lars Creutz (Trier University of Applied Sciences, Germany), Jens Schneider (Trier University of Applied Sciences, Germany), and Guido Dartmann (Trier University of Applied Sciences, Germany)

Situational Awareness for Smart Home IoT Security via Finite State Automata Based Attack Modeling 61
Fathima James (University of Missouri–Kansas City, USA), Indrajit Ray (Colorado State University, USA), and Deep Medhi (University of Missouri–Kansas City, USA)

Edge Centric Secure Data Sharing with Digital Twins in Smart Ecosystems 70
Glen Cathey (Tennessee Technological University, USA), James Benson (University of Texas at San Antonio, USA), Maanak Gupta (Tennessee Technological University, USA), and Ravi Sandhu (University of Texas at San Antonio, USA)

Research Session 3

A Comparative Evaluation of Differentially Private Image Obfuscation 80
Dominick Reilly (University of North Carolina at Charlotte) and Liyue Fan (University of North Carolina at Charlotte)

Can Pre-Trained Transformers be used in Detecting Complex Sensitive Sentences? - A Monsanto Case Study 90
Roelien C. Timmer (University of New South Wales, Australia), David Liebowitz (Penten UNSW Sydney, Australia), Surya Nepal (Data61 Cyber Security CRC, Australia), and Salil S. Kanhere (University of New South Wales, Australia)

Make Consumers Happy by Defuzzifying the Service Level Agreements 98
Kritagya Upadhyay (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Yanyan He (University of North Texas, USA), Abiola Salau (University of North Texas, USA), and Syed Badruddoja (University of North Texas, USA)

Application Session 1

Asynchronous Advantage Actor-Critic (A3C) Learning for Cognitive Network Security 106
Eric Muhati (Howard University) and Danda B. Rawat (Howard University)

Selective Targeted Transfer Learning for Malware Classification 114
Priyanka Aggarwal (Old Dominion University, USA), Sayyed F. Ahamed (Old Dominion University, USA), Sachin Shetty (Old Dominion University, USA), and Laura J. Freeman (Virginia Tech University, USA)

Homomorphic Encryption Reference Model for Mobile Cyber Physical Systems 121
Hassan Karim (Howard University, USA) and Danda B. Rawat (Howard University, USA)

Can't Understand SLAs? Use the Smart Contract 129
Kritagya Upadhyay (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Yanyan He (University of North Texas, USA), Syed Badruddoja (University of North Texas, USA), and Abiola Salau (University of North Texas, USA)

Vision Session 1

Security Challenges in the Container Cloud 137
Yutian Yang (Zhejiang University, China), Wenbo Shen (Zhejiang University, China), Bonan Ruan (NSFOCUS Inc., China), Wenmao Liu (NSFOCUS Inc., China), and Kui Ren (Zhejiang University, China)

Perception Poisoning Attacks in Federated Learning 146
Ka-Ho Chow (Georgia Institute of Technology, USA) and Ling Liu (Georgia Institute of Technology, USA)

Access Control Enforcement in IoT: State of the art and Open Challenges in the Zero Trust era 156
Pietro Colombo (University of Insubria, Italy), Elena Ferrari (University of Insubria, Italy), and Engin Deniz Tümer (University of Insubria, Italy)

Trustworthy and Sustainable Edge AI: A Research Agenda 164
Aaron Yi Ding (Delft University of Technology, Netherlands), Marijn Janssen (Delft University of Technology, Netherlands), and Jon Crowcroft (University of Cambridge, United Kingdom)

Deception for Cyber Defence: Challenges and Opportunities 173
David Liebowitz (Penten Pty Ltd, Australia; UNSW, Australia), Surya Nepal (Data61, CSIRO, Australia; Cyber Security Cooperative Research, Australia), Kristen Moore (Data61, CSIRO, Australia; Cyber Security Cooperative Research, Australia), Cody J. Christopher (Data61, CSIRO, Australia; Cyber Security Cooperative Research, Australia), Salil S. Kanhere (UNSW, Australia), David Nguyen (Data61, CSIRO, Australia; Cyber Security Cooperative Research, Australia; UNSW, Australia), Roelien C. Timmer (Data61, CSIRO, Australia; Cyber Security Cooperative Research, Australia; UNSW, Australia), Michael Longland (Data61, CSIRO, Australia; Cyber Security Cooperative Research, Australia; UNSW, Australia), and Keerth Rathakumar (Data61, CSIRO, Australia; Cyber Security Cooperative Research, Australia; UNSW, Australia)

Vision Session 2

DDoS Detection Systems for Cloud Data Storage 183
Ting Cao (Auburn University), Jianzhou Mao (Auburn University), Tathagata Bhattacharya (Auburn University), Xiaopu Peng (Auburn University), Wei-Shinn Ku (Auburn University), and Xiao Qin (Auburn University)

The Impact of Data Distribution on Fairness and Robustness in Federated Learning 191
Mustafa Safa Ozdayi (The University of Texas at Dallas, USA) and Murat Kantarcioglu (The University of Texas at Dallas, USA)

A Functional Model and Analysis of Next Generation Malware Attacks and Defenses 197
Calton Pu (Georgia Institute of Technology, USA), Qingyang Wang (Louisiana State University, USA), Yasuhiko Kanemasa (FUJITSU LIMITED, Japan), Rodrigo Alves Lima (Georgia Institute of Technology, USA), Joshua Kimball (Georgia Institute of Technology, USA), Shungeng Zhang (Augusta University, USA), Jianshu Liu (Louisiana State University, USA), and Xuhang Gu (Louisiana State University, USA)

The TSC-PFed Architecture for Privacy-Preserving FL 207
Stacey Truex (Denison University), Ling Liu (Georgia Institute of Technology), Mehmet Emre Gursoy (Koc University), Wenqi Wei (Georgia Institute of Technology), and Ka Ho Chow (Georgia Institute of Technology)

DDoS-as-a-Smokescreen: Leveraging Netflow Concurrency and Segmentation for Faster Detection 217
Brian Ricks (University of Texas at Dallas, USA), Patrick Tague (Carnegie Mellon University, USA), and Bhavani Thuraisingham (University of Texas at Dallas, USA)

Vision Session 3

The Evolving Path of “the Right to Be Left Alone” - When Privacy Meets Technology 225
Michela Iezzi (Bank of Italy, Italy)

Foundations for Robust Data Protection: Co-Designing Law and Computer Science 235
Kobbi Nissim (Georgetown University) and Alexandra Wood (Harvard University)

Towards Efficient Evaluation of ABAC Policies Using High-Dimensional Indexing Techniques 243
Proteet Paul (Indian Institute of Technology Kharagpur, India) and Shamik Sural (Indian Institute of Technology Kharagpur, India)

Energy-Aware Privacy Controls for Clouds 252
Jianzhou Mao (Auburn University), Ting Cao (Auburn University), Xiaopu Peng (Auburn University), Tathagata Bhattacharya (Auburn University), Wei-Shinn Ku (Auburn University), and Xiao Qin (Auburn University)

Paradigm Shift from Paper Contracts to Smart Contracts 261
Kritagya Upadhyay (University of North Texas, USA), Ram Dantu (University of North Texas, USA), Yanyan He (University of North Texas, USA), Abiola Salau (University of North Texas, USA), and Syed Badruddoja (University of North Texas, USA)

Vision Session 4

Online Symbolic Learning of Policies for Explainable Security 269
Arthur Drozdov (Imperial College London, United Kingdom), Mark Law (ILASP Limited, United Kingdom), Jorge Lobo (ICREA & Universitat Pompeu Fabra, Spain), Alessandra Russo (Imperial College London, United Kingdom), and Mercion Wilathgamuwage Don (Cisco Systems, Norway)

Towards Privacy in Deep Learning 279
Florian Kerschbaum (University of Waterloo, Canada)

Metaverse: Security and Privacy Issues 281
Roberto Di Pietro (Hamad Bin Khalifa University, Qatar) and Stefano Cresci (National Research Council, Italy)

Deep Transfer Learning for Physical Layer Security in Wireless Communication Systems 289
Danda B. Rawat (Howard University, USA)

Securing social media for seniors from information attacks: Modeling, detecting, intervening, and communicating risks 297
Vignesh Narayanan (University of South Carolina), Brett W. Robertson (University of South Carolina), Andrea Hickerson (University of South Carolina), Biplav Srivastava (University of South Carolina), and Bryant W. Smith (University of South Carolina)

Similarities and Learnings from Ancient Literature on Blockchain Consensus and Integrity 303
Ashish Kundu (Cisco Research), Arun Ayachitula (Kyndryl), and Nagamani Sistla (Freelance Researcher)

AI-Driven Selective Protection of Multimedia Data 307
Ashish Kundu (Cisco Research), Abhishek Reddypalle (IIIT Sricity), and Chinmay Kundu (KIIT University)

Agriculture Cyber Security - Session 1

Traceable, Trustworthy and Privacy Preserving Agri-Food Supply Chains 313
Sidra Malik (UNSW, Sydney, Australia), Volkan Dedeoglu (CSIRO Data61, Australia), Salil S. Kanhere (UNSW, Sydney, Australia), Raja Jurdak (QUT, Brisbane, Australia), and Hye-Young Paik (UNSW, Sydney, Australia)

Towards Assisted Autonomy for Supply Chain Compliance Management 321
Gowri Sankar Ramachandran (Queensland University of Technology, Australia), Felicity Deane (Queensland University of Technology, Australia), Sidra Malik (Queensland University of Technology, Australia), Ali Dorri (Queensland University of Technology, Australia), and Raja Jurdak (Queensland University of Technology, Australia)

Blockchain Technology: A Case Study in Supply Chain Management 331
Taha Abdelgalil (University of West Attica, Greece), Vasileios Manolas (University of West Attica, Greece), Leandros Maglaras (De Montfort University, UK), Ioanna Kantzavelou (University of West Attica, Greece), and Mohamed Amine Ferrag (University of Guelma, Algeria)

Agriculture Cyber Security - Session 2

A Privacy Preserving Anomaly Detection Framework for Cooperative Smart Farming Ecosystem .. 340
Sai Sree Laya Chukkapalli (University of Maryland Baltimore County, USA), Priyanka Ranade (University of Maryland Baltimore County, USA), Sudip Mittal (Mississippi State University, USA), and Anupam Joshi (University of Maryland Baltimore County, USA)

A Laboratory-Scale Canal SCADA System Testbed for Cybersecurity Research 348
Mohammad E. Alim (University of Alabama in Huntsville, USA), Shelton R. Wright (University of Alabama in Huntsville, USA), and Tommy H. Morris (University of Alabama in Huntsville, USA)

Modeling Multi-Layer Access Control Policies of a Hyperledger-Fabric-Based Agriculture Supply Chain 355
H.M.N. Dilum Bandara (Data61, CSIRO, Australia), Shiping Chen (Data61, CSIRO, Australia), Mark Staples (Data61, CSIRO, Australia), and Yilin Sai (Data61, CSIRO, Australia)

Author Index **365**