

2021 18th International Conference on Privacy, Security and Trust (PST 2021)

**Auckland, New Zealand
13 – 15 December 2021**



**IEEE Catalog Number: CFP2104F-POD
ISBN: 978-1-6654-0185-2**

**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:	CFP2104F-POD
ISBN (Print-On-Demand):	978-1-6654-0185-2
ISBN (Online):	978-1-6654-0184-5

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

EPSIM-GS: EFFICIENT AND PRIVACY-PRESERVING SIMILARITY RANGE QUERY OVER GENOMIC SEQUENCES.....	1
<i>Jiacheng Jin, Yandong Zheng, Pulei Xiong</i>	
AN EFFECTIVE INTRUSION DETECTION MODEL FOR CLASS-IMBALANCED LEARNING BASED ON SMOTE AND ATTENTION MECHANISM	11
<i>Xubin Jiao, Jinguo Li</i>	
FOX: FOOLING WITH EXPLANATIONS - PRIVACY PROTECTION WITH ADVERSARIAL REACTIONS IN SOCIAL MEDIA	17
<i>Noreddine Belhadj-Cheikh, Abdessamad Imine, Michaël Rusinowitch</i>	
A WEARABLES-DRIVEN ATTACK ON EXAMINATION PROCTORING	27
<i>Tasnia Ashrafi Heya, Abdul Serwadda, Isaac Griswold-Steiner, Richard Matovu</i>	
TRUST QUANTIFICATION FOR AUTONOMOUS MEDICAL ADVISORY SYSTEMS	34
<i>Mini Thomas, Reza Samavi, Thomas E. Doyle</i>	
DETECTION OF DEMAND MANIPULATION ATTACKS ON A POWER GRID	41
<i>Srinidhi Madabhushi, Rinku Dewri</i>	
DAZED AND CONFUSED: WHAT'S WRONG WITH CRYPTO LIBRARIES?	48
<i>Mohammadreza Hazhirpasand, Oscar Nierstrasz, Mohammad Ghafari</i>	
USING CGAN TO DEAL WITH CLASS IMBALANCE AND SMALL SAMPLE SIZE IN CYBERSECURITY PROBLEMS	54
<i>Ehsan Nazari, Paula Branco, Guy-Vincent Jourdan</i>	
FORTRESS: FORTIFIED TAMPER-RESISTANT ENVELOPE WITH EMBEDDED SECURITY SENSOR.....	64
<i>Kathrin Garb, Johannes Obermaier, Elischa Ferres, Martin Küning</i>	
SEARCHING ON NON-SYSTEMATIC ERASURE CODES	76
<i>Atthapan Daramas, Vimal Kumar</i>	
A LARGE-SCALE SECURITY-ORIENTED STATIC ANALYSIS OF PYTHON PACKAGES IN PYPI	84
<i>Jukka Ruohonen, Kalle Hjerppe, Kalle Rindell</i>	
LIGHT-WEIGHT ACTIVE SECURITY FOR DETECTING DDOS ATTACKS IN CONTAINERISED ICPS.....	94
<i>Farzana Zahid, Matthew M. Y. Kuo, Roopak Sinha</i>	
BALANCING EFFICIENCY AND SECURITY FOR NETWORK ACCESS CONTROL IN SPACE-AIR-GROUND INTEGRATED NETWORKS	99
<i>Miao He, Xiangman Li, Jianbing Ni, Haomiao Yang</i>	
STEELEYE: AN APPLICATION-LAYER ATTACK DETECTION AND ATTRIBUTION MODEL IN INDUSTRIAL CONTROL SYSTEMS USING SEMI-DEEP LEARNING	109
<i>Sanaz Nakhodchi, Behrouz Zolfaghari, Abbas Yazdinejad, Ali Dehghantanha</i>	

API-BASED RANSOMWARE DETECTION USING MACHINE LEARNING-BASED THREAT DETECTION MODELS	117
<i>May Almousa, Sai Basavaraju, Mohd Anwar</i>	
UPDATABLE LINEAR MAP COMMITMENTS AND THEIR APPLICATIONS IN ELEMENTARY DATABASES.....	124
<i>Guiwen Luo, Shihui Fu, Guang Gong</i>	
MEASUREMENT OF LOCAL DIFFERENTIAL PRIVACY TECHNIQUES FOR IOT-BASED STREAMING DATA.....	130
<i>Sharmin Afrose, Danfeng Daphne Yao, Olivera Kotevska</i>	
TOWARDS QUERY-EFFICIENT BLACK-BOX ADVERSARIAL ATTACK ON TEXT CLASSIFICATION MODELS	140
<i>Mohammad Mehdi Yadollahi, Arash Habibi Lashkari, Ali A. Ghorbani</i>	
A PRACTICAL OBLIVIOUS CLOUD STORAGE SYSTEM BASED ON TEE AND CLIENT GATEWAY	147
<i>Wensheng Zhang</i>	
DETERMINISTIC AND STATISTICAL STRATEGIES TO PROTECT ANNS AGAINST FAULT INJECTION ATTACKS	153
<i>Troya Çagil Köylü, Cezar Rodolfo Wedig Reinbrecht, Said Hamdioui, Mottaqiallah Taouil</i>	
DAROUTE: INFERRING TRAJECTORIES FROM ZERO-PERMISSION SMARTPHONE SENSORS	163
<i>Christian Roth, Ngoc Thanh Dinh, Marc Roßberger, Dogan Kesdogan</i>	
GAIROSCOPE: LEAKING DATA FROM AIR-GAPPED COMPUTERS TO NEARBY SMARTPHONES USING SPEAKERS-TO-GYRO COMMUNICATION	173
<i>Mordechai Guri</i>	
INTRODUCING A FRAMEWORK TO ENABLE ANONYMOUS SECURE MULTI-PARTY COMPUTATION IN PRACTICE.....	183
<i>Malte Breuer, Ulrike Meyer, Susanne Wetzel</i>	
USER IDENTIFICATION IN ONLINE SOCIAL NETWORKS USING GRAPH TRANSFORMER NETWORKS	190
<i>K. N. Pavan Kumar, Marina L. Gavrilova</i>	
LIBBLOCK - TOWARDS DECENTRALIZED LIBRARY SYSTEM BASED ON BLOCKCHAIN AND IPFS	200
<i>Wei-Yang Chiu, Weizhi Meng, Wenjuan Li</i>	
DESIGNING PERSONALIZED OS UPDATE MESSAGE BASED ON SECURITY BEHAVIOR STAGE MODEL	209
<i>Ayane Sano, Yukiko Sawaya, Akira Yamada, Ayumu Kubota, Takamasa Isohara</i>	
CLUSTERING BASED OPCODE GRAPH GENERATION FOR MALWARE VARIANT DETECTION.....	218
<i>Fok Kar Wai, Vrizlynn L. L. Thing</i>	
DATA PRIVACY IN MULTI-CLOUD: AN ENHANCED DATA FRAGMENTATION FRAMEWORK.....	229
<i>Randolph Loh, Vrizlynn L. L. Thing</i>	

TOWARDS PRIVACY-FRIENDLY SMART PRODUCTS	234
<i>Kimberly García, Zaira Zihlmann, Simon Mayer, Aurelia Tamò-Larrieux, Johannes Hooss</i>	
TOWARDS PRIVACY-PRESERVING CLASSIFICATION-AS-A-SERVICE FOR DGA DETECTION.....	241
<i>Arthur Drichel, Mehdi Akbari Gurabi, Tim Amelung, Ulrike Meyer</i>	
A HYBRID SECURE COMPUTATION FRAMEWORK FOR GRAPH NEURAL NETWORKS.....	251
<i>Yixuan Ren, Yixin Jie, Qingtao Wang, Bingbing Zhang, Chi Zhang, Lingbo Wei</i>	
THE RACE-TIMING PROTOTYPE.....	257
<i>Andrés R. Hernández C, Wonjun Lee, Wei-Ming Lin</i>	
EPF: AN EVOLUTIONARY, PROTOCOL-AWARE, AND COVERAGE-GUIDED NETWORK FUZZING FRAMEWORK	267
<i>René Helmke, Eugen Winter, Michael Rademacher</i>	
CLEAR THE FOG: TOWARDS A TAXONOMY OF SELF-SOVEREIGN IDENTITY ECOSYSTEM MEMBERS.....	274
<i>Kaja Schmidt, Alexander Mühle, Andreas Grüner, Christoph Meinel</i>	
PREPARING FOR NATIONAL CYBER CRISES USING NON-LINEAR CYBER EXERCISES	281
<i>Florian Skopik, Maria Leitner</i>	
USER PROFILING ON UNIVERSAL DATA INSIGHTS TOOL ON IBM CLOUD PAK FOR SECURITY	286
<i>Farzaneh Shoeleh, Masoud Erfani, Saeed Shafeiee Hasanabadi, Duc-Phong Le, Arash Habibi Lashkari, Adam Frank, Ali A. Ghorbani</i>	
A NOVEL TRUST MODEL IN DETECTING FINAL-PHASE ATTACKS IN SUBSTATIONS	296
<i>Kwasi Boakye-Boateng, Ali A. Ghorbani, Arash Habibi Lashkari</i>	
SECURING CRITICAL INFRASTRUCTURE THROUGH INNOVATIVE USE OF MERGED HIERARCHICAL DEEP NEURAL NETWORKS	307
<i>Lav Gupta</i>	
INTRUSION DETECTION IN INTERNET OF THINGS USING CONVOLUTIONAL NEURAL NETWORKS.....	315
<i>Martin Kodyš, Zhi Lu, Kar Wai Fok, Vrizzlynn L. L. Thing</i>	
PIDARCI: USING ASSEMBLY INSTRUCTION PATTERNS TO IDENTIFY, ANNOTATE, AND REVERT COMPILER IDIOMS.....	325
<i>Steffen Enders, Mariia Rybalka, Elmar Padilla</i>	
CROSS THE CHASM: SCALABLE PRIVACY-PRESERVING FEDERATED LEARNING AGAINST POISONING ATTACK.....	332
<i>Yiran Li, Guiqiang Hu, Xiaoyuan Liu, Zuobin Ying</i>	
TOWARDS CHANGE DETECTION IN PRIVACY POLICIES WITH NATURAL LANGUAGE PROCESSING.....	337
<i>Andrick Adhikari, Rinku Dewri</i>	
IMPACT OF ENVIRONMENTAL CONDITIONS ON FINGERPRINT SYSTEMS PERFORMANCE	347
<i>Abdarahmane Wone, Joël Di Manno, Christophe Charrier, Christophe Rosenberger</i>	

DEEP FEDERATED LEARNING-BASED CYBER-ATTACK DETECTION IN INDUSTRIAL CONTROL SYSTEMS	352
<i>Amir Namavar Jahromi, Hadis Karimipour Schulich, Ali Dehghantanha</i>	
PUPY: A GENERALIZED, OPTIMISTIC CONTEXT DETECTION FRAMEWORK FOR IMPLICIT AUTHENTICATION.....	358
<i>Matthew Rafuse, Urs Hengartner</i>	
A NEW APPROACH FOR CROSS-SILO FEDERATED LEARNING AND ITS PRIVACY RISKS.....	368
<i>Michele Fontana, Francesca Naretto, Anna Monreale</i>	
EPISTEMIC ANALYSIS OF A KEY-MANAGEMENT VULNERABILITY IN LORAWAN	378
<i>Martha N. Kamkuemah</i>	
LONG PASSPHRASES: POTENTIALS AND LIMITS	385
<i>Christopher Bonk, Zach Parish, Julie Thorpe, Amirali Salehi-Abari</i>	
EVALUATING THE CURRENT STATE OF APPLICATION PROGRAMMING INTERFACES FOR VERIFIABLE CREDENTIALS	392
<i>Nikesh Lalchandani, Frank Jiang, Jongkil Jay Jeong, Yevhen Zolotavkin, Robin Doss</i>	
SEGMENTPERTURB: EFFECTIVE BLACK-BOX HIDDEN VOICE ATTACK ON COMMERCIAL ASR SYSTEMS VIA SELECTIVE DELETION.....	399
<i>Ganyu Wang, Miguel Vargas Martin</i>	
GAINING LOCATION PRIVACY FROM SERVICE FLEXIBILITY: A BAYESIAN GAME THEORETIC APPROACH.....	411
<i>Shu Hong, Lingjie Duan, Jianwei Huang</i>	
UNMASKING PRIVACY LEAKAGE THROUGH ANDROID APPS OBSCURED WITH HIDDEN PERMISSIONS.....	421
<i>Pranav Kotak, Shweta Bhandari, Akka Zemmari, Jaykrishna Joshi</i>	
TEE-BASED SELECTIVE TESTING OF LOCAL WORKERS IN FEDERATED LEARNING SYSTEMS.....	426
<i>Wensheng Zhang, Trent Muhr</i>	
FOOL ME ONCE: A STUDY OF PASSWORD SELECTION EVOLUTION OVER THE PAST DECADE.....	432
<i>Rahul Dubey, Miguel Vargas Martin</i>	
DELETION-COMPLIANCE IN THE ABSENCE OF PRIVACY	439
<i>Jonathan Godin, Philippe Lamontagne</i>	
PRACTICAL PROTECTION OF BINARY APPLICATIONS VIA TRANSPARENT IMMUNIZATION.....	449
<i>Xinyuan Wang</i>	
TRACEABLE AND PRIVACY-PRESERVING NON-INTERACTIVE DATA SHARING IN MOBILE CROWDSENSING	456
<i>Fuyuan Song, Zheng Qin, Jinwen Liang, Pulei Xiong, Xiaodong Lin</i>	
DETECTION OF INDUCED FALSE NEGATIVES IN MALWARE SAMPLES.....	465
<i>Adrian Wood, Michael N. Johnstone</i>	

SECURE ALLOCATION FOR GRAPH-BASED VIRTUAL MACHINES IN CLOUD ENVIRONMENTS 471
Mansour Aldawood, Arshad Jhumka

IOT MALWARE DETECTION USING FUNCTION-CALL-GRAPH EMBEDDING 478
Chia-Yi Wu, Tao Ban, Shin-Ming Cheng, Bo Sun, Takeshi Takahashi

Author Index