

# **2021 IEEE Conference on Dependable and Secure Computing (DSC 2021)**

**Aizuwakamatsu, Fukushima, Japan  
30 January – 2 February 2021**



**IEEE Catalog Number: CFP21J65-POD**  
**ISBN: 978-1-7281-7535-5**

**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:	CFP21J65-POD
ISBN (Print-On-Demand):	978-1-7281-7535-5
ISBN (Online):	978-1-7281-7534-8

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# TABLE OF CONTENTS

<b>HIGHLY EFFICIENT ANONYMOUS IOT AUTHENTICATION USING COMPOSITE HASHING</b> .....	1
<i>Hung-Yu Chien</i>	
<b>HEADER-TRANSLATION BASED FLOW AGGREGATION FOR SCATTERED ADDRESS ALLOCATING SDNS</b> .....	8
<i>Ruisi Wu; Wen-Kang Jia; Xufang Wang</i>	
<b>ATTRIBUTE-BASED SEARCHABLE ENCRYPTION SCHEME SUPPORTING EFFICIENT RANGE SEARCH IN CLOUD COMPUTING</b> .....	16
<i>Yuan Li; Haiyan Wang; Shulan Wang; Yong Ding</i>	
<b>MIXED-MODE INFORMATION FLOW TRACKING WITH COMPILE-TIME TAINT SEMANTICS EXTRACTION AND OFFLINE REPLAY</b> .....	24
<i>Yu-Hsin Hung; Bing-Jhong Jheng; Hong-Wei Li; Wen-Yang Lai; Sanoop Mallisery; Yu-Sung Wu</i>	
<b>A REINFORCED DYNAMIC MULTI-KEYWORD RANKED SEARCH WITH FORWARD PRIVACY</b> .....	32
<i>Chien-Ming Chen; Zhuoyu Tie; Eric Ke Wang; Kuo-Hui Yeh; Wensheng Gan; S. K. Hafizul Islam</i>	
<b>EFFICIENT SUBSET PREDICATE ENCRYPTION FOR INTERNET OF THINGS</b> .....	40
<i>Yi-Fan Tseng; Shih-Jie Gao</i>	
<b>DECENTRALIZED DATA AGGREGATION: A NEW SECURE FRAMEWORK BASED ON LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS</b> .....	42
<i>Xin Xie; Yu-Chi Chen</i>	
<b>PRIVACY-PRESERVING SMART ROAD PRICING SYSTEM IN SMART CITIES</b> .....	44
<i>Qingfeng Zhu; Sai Ji; Qi Liu</i>	
<b>AN EFFICIENT ANONYMOUS AUTHENTICATION SCHEME FOR PRIVACY-PRESERVING IN SMART GRID</b> .....	46
<i>Xueya Xia; Sai Ji</i>	
<b>FASTMOVE: FAST IP SWITCHING MOVING TARGET DEFENSE TO MITIGATE DDOS ATTACKS</b> .....	48
<i>Nahid Bandi; Hesam Tajbakhsh; Morteza Analoui</i>	
<b>A NOVEL DYNAMIC GROUP SIGNATURE WITH MEMBERSHIP PRIVACY</b> .....	55
<i>Junqing Lu; Rongxin Qi; Jian Shen</i>	
<b>A PROFILE MATCHING SCHEME BASED ON PRIVATE SET INTERSECTION FOR CYBER-PHYSICAL-SOCIAL SYSTEMS</b> .....	60
<i>Yalian Qian; Xueya Xia; Jian Shen</i>	
<b>A PROVABLE DATA POSSESSION PROTOCOL IN CLOUD STORAGE SYSTEMS WITH FAULT TOLERANCE</b> .....	65
<i>Kui Zhu; Yongjun Ren; Qingfeng Zhu</i>	
<b>TOWARD BLOCKCHAIN-ENABLED IOV WITH EDGE COMPUTING: EFFICIENT AND PRIVACY-PRESERVING VEHICULAR COMMUNICATION AND DYNAMIC UPDATING</b> .....	71
<i>Qian Mei; Hu Xiong; Yanan Zhao; Kuo-Hui Yeh</i>	
<b>PARTIALLY BLIND ECDSA SCHEME AND ITS APPLICATION TO BITCOIN</b> .....	79
<i>Hongxun Huang; Zi-Yuan Liu; Raylin Tso</i>	
<b>DBMS-FRIENDLY SEARCHABLE SYMMETRIC ENCRYPTION: CONSTRUCTING INDEX GENERATION SUITABLE FOR DATABASE MANAGEMENT SYSTEMS</b> .....	87
<i>Takato Hirano; Yutaka Kawai; Yoshihiro Koseki</i>	
<b>A PATIENT-CENTRIC KEY MANAGEMENT PROTOCOL FOR HEALTHCARE INFORMATION SYSTEM BASED ON BLOCKCHAIN</b> .....	95
<i>Ting-Le Zhu; Tzung-Her Chen</i>	
<b>ON THE CONSTRUCTION OF A POST-QUANTUM BLOCKCHAIN</b> .....	100
<i>Jiahui Chen; Wensheng Gan; Muchuang Hu; Chien-Ming Chen</i>	
<b>ARITHMETIC CODING FOR FLOATING-POINT NUMBERS</b> .....	108
<i>Marc Fischer; Oliver Riedel; Armin Lechler; Alexander Verl</i>	
<b>GENERATE REALISTIC TRAFFIC SIGN IMAGE USING DEEP CONVOLUTIONAL GENERATIVE ADVERSARIAL NETWORKS</b> .....	116
<i>Yan-Ting Liu; Rung-Ching Chen; Christine Dewi</i>	
<b>USING GENERATIVE ADVERSARIAL NETWORKS FOR DATA AUGMENTATION IN ANDROID MALWARE DETECTION</b> .....	122
<i>Yi-Ming Chen; Chun-Hsien Yang; Guo-Chung Chen</i>	

<b>MINING WEB USAGE PROFILES FROM PROXY LOGS: USER IDENTIFICATION</b> .....	130
<i>Jing Xu; Fei Xu; Fanshu Ma; Lei Zhou; Shuanglin Jiang; Zhibo Rao</i>	
<b>IOT ETEI: END-TO-END IOT DEVICE IDENTIFICATION METHOD</b> .....	136
<i>Feihong Yin; Li Yang; Yuchen Wang; Jiahao Dai</i>	
<b>DESIGNATED VERIFIER SIGNATURE TRANSFORMATION: A NEW FRAMEWORK FOR ONE-TIME DELEGATING VERIFIABILITY</b> .....	144
<i>Jian-Feng Lin; Jun-Rui Wang; Che-Chia Chang; Yu-Chi Chen</i>	
<b>SGD<sup>2</sup>: SECURE GROUP-BASED DEVICE-TO-DEVICE COMMUNICATIONS WITH FINE-GRAINED ACCESS CONTROL FOR IOT IN 5G</b> .....	146
<i>Ruei-Hau Hsu; Hsiang-Shian Fan; Lu-Chin Wang</i>	
<b>CCA-SECURE ATTRIBUTE-BASED ENCRYPTION SUPPORTING DYNAMIC MEMBERSHIP IN THE STANDARD MODEL</b> .....	154
<i>Chun-I Fan; Yi-Fan Tseng; Cheng-Chun Feng</i>	
<b>BDF-SDN: A BIG DATA FRAMEWORK FOR DDOS ATTACK DETECTION IN LARGE-SCALE SDN-BASED CLOUD</b> .....	162
<i>Phuc Trinh Dinh; Minh Park</i>	
<b>ENHANCING CHALLENGE-BASED COLLABORATIVE INTRUSION DETECTION AGAINST INSIDER ATTACKS USING SPATIAL CORRELATION</b> .....	170
<i>Wenjuan Li; Weizhi Meng; Javier Parra-Arnau; Kim-Kwang Raymond Choo</i>	
<b>VERIFIABLE M-LST-PRICE AUCTION WITHOUT MANAGER</b> .....	178
<i>Po-Chu Hsu; Atsuko Miyaji</i>	
<b>SMART MARKERS IN SMART CONTRACTS: ENABLING MULTIWAY BRANCHING AND MERGING IN BLOCKCHAIN FOR DECENTRALIZED RUNTIME VERIFICATION</b> .....	186
<i>Tieming Geng; Laurent Njilla; Chin-Tser Huang</i>	
<b>A BLACK-BOX ADVERSARIAL ATTACK VIA DEEP REINFORCEMENT LEARNING ON THE FEATURE SPACE</b> .....	194
<i>Lyue Li; Amir Rezapour; Wen-Guey Tzeng</i>	
<b>PRIVACY-PRESERVING RANGE QUERY FOR HIGH-DIMENSIONAL UNCERTAIN DATA IN A TWO-PARTY SCENARIO</b> .....	201
<i>Su Shenghao; Guo Cheng; Tian Pengxu; Tang Xinyu</i>	
<b>ON THE SECURITY OF PERMISSIONLESS BLOCKCHAIN SYSTEMS: CHALLENGES AND RESEARCH PERSPECTIVE</b> .....	208
<i>Hao Wang; Chunpeng Ge; Zhe Liu</i>	
<b>SYSTEMATIC RESEARCH ON TECHNOLOGY AND CHALLENGES OF LIGHTNING NETWORK</b> .....	216
<i>Zhixin Zhao; Lu Zhou; Chunhua Su</i>	
<b>EC-MODEL: AN EVOLVABLE MALWARE CLASSIFICATION MODEL</b> .....	224
<i>Shan-Hsin Lee; Shen-Chieh Lan; Hsiu-Chuan Huang; Chia-Wei Hsu; Yung-Shiu Chen; Shihpyng Shieh</i>	
<b>A PUBLIC-KEY ENCRYPTION WITH MULTI-KEYWORD SEARCH SCHEME FOR CLOUD-BASED SMART GRIDS</b> .....	232
<i>Dong Zhang; Qing Fan; Hongyi Qiao; Min Luo</i>	
<b>VULNERABILITY OF PRIVACY VISOR USED TO DISRUPT UNAUTHORIZED FACE RECOGNITION</b> .....	238
<i>Hiroaki Kikuchi; Kazuki Eto; Kazushi Waki; Takafumi Mori</i>	
<b>A DISTRIBUTED LEDGER MANAGEMENT MECHANISM FOR STORING AND SELLING PRIVATE DATA</b> .....	245
<i>Sabyasachi Dutta; Arinjita Paul; Rocki H. Ozaki; C. Pandu Ranzan; Kouichi Sakurai</i>	
<b>CHAINPKI - TOWARDS ETHASH-BASED DECENTRALIZED PKI WITH PRIVACY ENHANCEMENT</b> .....	253
<i>Wei-Yang Chiu; Weizhi Meng; Christian D. Jensen</i>	
<b>EFFICIENT BLOCKCHAIN-BASED IOT FIRMWARE UPDATE CONSIDERING DISTRIBUTION INCENTIVES</b> .....	261
<i>Tatsuhiko Fukuda; Kazumasa Omote</i>	
<b>SECURE OUTSOURCED PRIVATE SET INTERSECTION WITH LINEAR COMPLEXITY</b> .....	269
<i>Sumit Kumar Debnath; Kouchi Sakurai; Kunal Dey; Nibedita Kundu</i>	
<b>A CERTIFICATELESS AND PRIVACY-PRESERVING AUTHENTICATION WITH FAULT-TOLERANCE FOR VEHICULAR SENSOR NETWORKS</b> .....	277
<i>Yang Zhao; Guohang Dan; Ankang Ruan; Jicheng Huang; Hu Xiong</i>	
<b>EFFICIENT MULTI-AUTHORITY ATTRIBUTE-BASED SIGNCRYPTION WITH CONSTANT-SIZE CIPHERTEXT</b> .....	284
<i>Yang Zhao; Ankang Ruan; Guohang Dan; Jicheng Huang; Yi Ding</i>	

<b>PERPETUAL SECRET SHARING FROM DYNAMIC DATA STRUCTURES</b> .....	292
<i>Shion Samadder Chaudhury; Sabyasachi Dutta; Kouichi Sakurai</i>	
<b>DUALNET: LOCATE THEN DETECT EFFECTIVE PAYLOAD WITH DEEP ATTENTION NETWORK</b> .....	300
<i>Shiyi Yang; Peilun Wu; Hui Guo</i>	
<b>A NOVEL VERIFICATION SCHEME FOR RESISTING PASSWORD GUESSING ATTACKS</b> .....	308
<i>Albert Guan; Chia-Mei Chen</i>	
<b>RETRIEVING INPUT FROM TOUCH INTERFACES VIA ACOUSTIC EMANATIONS</b> .....	310
<i>Kai Ren Teo; B. T. Balamurali; Chen Jer Ming; Jianying Zhou</i>	
<b>CRYFIND: USING STATIC ANALYSIS TO IDENTIFY CRYPTOGRAPHIC ALGORITHMS IN BINARY EXECUTABLES</b> .....	318
<i>Wei Chieh Chao; Chung-Kuan Chen; Chen-Mou Cheng</i>	
<b>PHISHING SITE DETECTION USING SIMILARITY OF WEBSITE STRUCTURE</b> .....	320
<i>Shoma Tanaka; Takashi Matsunaka; Akira Yamada; Avumu Kubota</i>	
<b>EXAMCHAIN: A PRIVACY-PRESERVING ONSCREEN MARKING SYSTEM BASED ON CONSORTIUM BLOCKCHAIN</b> .....	328
<i>Haoyang An; Jiageng Chen</i>	
<b>Author Index</b>	