2023 18th Asia Joint Conference on Information Security (AsiaJCIS 2023)

Tokyo, Japan
15-16 August 2023

IEEE Catalog Number: CFP2333T-POD
ISBN: 979-8-3503-4164-5

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:	CFP2333T-POD
ISBN (Print-On-Demand):	979-8-3503-4164-5
ISBN (Online):	979-8-3503-4163-8
ISSN:	2374-0205

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

2023 18th Asia Joint Conference on Information Security (AsiaJCIS)

AsiaJCIS 2023

Table of Contents

Message from the General Co-Chairs ..... **viii**
Message from the Program Co-Chairs ..... **ix**
Organizing Committee ..... **x**
Technical Program Committee ..... **xi**
Steering Committee ..... **xiii**
Reviewers ..... **xiv**
Sponsors and Supporters ..... **xv**

Regular Papers

VMI System with Smart Contracts for Demand Forecasting 1
Kenta Hagiwara (University of Tsukuba, Japan) and Kazumasa Omote (University of Tsukuba, National Institute of Information and Communications Technology, Japan)

Receipt-Freeness By Flexible Usage Of Mix Network 9
Kun Peng (Huawei Technology)

A Revocation Key-Based Approach Towards Efficient Federated Unlearning 17
Rui-Zhen Xu (National Taiwan Normal University, Taiwan), Sheng-Yi Hong (National Taiwan Normal University, Taiwan), Po-Wen Chi (National Taiwan Normal University, Taiwan), and Ming-Hung Wang (National Chung Cheng University, Taiwan)

A Novel Ciphertext-Policy Attribute-Based Encryption Supporting Dual Membership 25
Yi-Fan Tseng (National Chengchi University, Taiwan), Jheng-Jia Huang (National Taiwan University of Science and Technology, Taiwan), Guan-Yu Chen (National Taiwan University of Science and Technology, Taiwan), Wei-Hsueh Wang (National Taiwan University of Science and Technology, Taiwan), Yi-Hsueh Lu (National Chengchi University, Taiwan), Wen-Yi Chen (National Chengchi University, Taiwan), and Shih-Pei Kao (National Chengchi University, Taiwan)

Intrusion Detection Systems Based on Machine Learning using Feature Expansion Methods 32
Joonwoo Myung (Science and Technology Security R&D Center, Korea Institute of Science and Technology Information, Daejeon, Republic of Korea), Youngmin Ko (Science and Technology Security R&D Center, Korea Institute of Science and Technology Information, Daejeon, Republic of Korea), Taewoong Kwon (Science and Technology Security R&D Center, Korea Institute of Science and Technology Information, Daejeon, Republic of Korea), Jun Lee (Science and Technology Security R&D Center, Korea Institute of Science and Technology Information, Daejeon, Republic of Korea), Kyuil Kim (Science and Technology Security R&D Center, Korea Institute of Science and Technology Information, Daejeon, Republic of Korea), and Jungsuk Song (Science and Technology Security R&D Center, Korea Institute of Science and Technology Information, Daejeon, Republic of Korea)

Towards Privacy-Preserving and Practical Vaccine Supply Chain Based on Blockchain 39
Baodong Wen (Guilin University of Electronic Technology, China), Yujue Wang (Hangzhou Innovation Institute of Beihang University, China), Yong Ding (Guilin University of Electronic Technology; Cyberspace Security Research Center, Pengcheng Laboratory, China), Hai Liang (Guilin University of Electronic Technology, China), Changsong Yang (Guilin University of Electronic Technology, China), and Decun Luo (Hangzhou Innovation Institute of Beihang University, China)

Privacy Preserving Provable Data Possession: A FHE-Based Hash Approach 47
Sheng-Yi Hong (National Taiwan Normal University, Taiwan), Rui-Zhen Xu (National Taiwan Normal University, Taiwan), Po-Wen Chi (National Taiwan Normal University, Taiwan), and Albert Guan (National Taiwan Normal University, Taiwan)

A secure firmware and software update model based on blockchains for Internet of Things devices using SBOM 53
Da Eun Hyeon (Soonchunhyang University, Korea), Jun Hyung Park (Soonchunhyang University, Korea), and Heung Youl Youm (Soonchunhyang University, Korea)

Short Papers

Development of the Edge Computing Platform Based on Modular Architecture using Intel SGX 59
Yuma Nishihira (Tokai University, Japan), Takuya Ishibashi (Tokai University, Japan), Yoshio Kakizaki (Tokai University, Japan), Toshihiro Ohigashi (Tokai University; National Institute of Information and Communications Technology (NICT), Japan), Hidenobu Watanabe (Hiroshima University, Japan), Tohru Kondo (Hiroshima University, Japan), and Reiji Aibara (Hiroshima University, Japan)

A Certificate Management Mechanism using Distributed Ledger 66
Iuon-Chang Lin (National Chung Hsing University, Taiwan), Jing-Yuan Huang (National Chung Hsing University, Taiwan), and Jason Lin (National Chung Hsing University, Taiwan)

Anonymous and Unlinkable Identity Scheme in Open Data Environment 73
Jheng-Jia Huang (National Taiwan University of Science and Technology, Taiwan), Wei-Hsueh Wang (National Taiwan University of Science and Technology, Taiwan), Yi-Fan Tseng (National Chengchi University, Taiwan), Guan-Yu Chen (National Taiwan University of Science and Technology, Taiwan), Hao-Hsiang Chang Chien (National Taiwan University of Science and Technology, Taiwan), Wen-Yan Dai (National Taiwan University of Science and Technology, Taiwan), and Nai-Wei Lo (National Taiwan University of Science and Technology, Taiwan)

Phishing Detection with Browser Extension Based on Machine Learning 81
Che-Yu Wu (National Cheng Kung University, Taiwan), Cheng-Chung Kuo (National Cheng Kung University, Taiwan), and Chu-Sing Yang (National Cheng Kung University, Taiwan)

Packet-Level Intrusion Detection using LSTM Focusing on Personal Information and Payloads 88
Shota Kawanaka (Kyushu University, Japan), Yoshikatsu Kashiwabara (Kyushu University, Japan), Kohei Miyamoto (National Institute of Information and Communications Technology, Japan), Masazumi Iida (Kyushu University, Japan), Chansu Han (National Institute of Information and Communications Technology; Kyushu University, Japan), Tao Ban (National Institute of Information and Communications Technology, Japan), Takeshi Takahashi (National Institute of Information and Communications Technology, Japan), and Jun'ichi Takeuchi (Kyushu University, Japan)

Revisited Linear Approximation Formula of ChaCha 95
Atuski Nagai (Osaka University, Japan) and Atsuko Miyaji (Osaka University, Japan)

Privacy-Preserving Frequency Estimation Method 102
Naoki Kawahara (Osaka University, Japan), Atsuko Miyaji (Osaka University, Japan), and Tomoaki Mimoto (KDDI Research, Inc., Japan)

Author Index **109**