2024 Silicon Valley Cybersecurity Conference (SVCC 2024)

Seoul, South Korea
17-19 June 2024

IEEE

IEEE Catalog Number: CFP24DI5-POD
ISBN: 979-8-3503-8315-7

****** 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:	CFP24DI5-POD
ISBN (Print-On-Demand):	979-8-3503-8315-7
ISBN (Online):	979-8-3503-8314-0

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

TABLE OF CONTENTS

Silent Sabotage: A Stealthy Control Logic Injection in IIoT Systems 1
Wael Alsabbagh, Chaerin Kim, Peter Langendörfer

Anomaly Detection in 5G Using Variational Autoencoders 9
Amanul Islam, Sang-Yoon Chang, Jinoh Kim, Jonghyun Kim

A Distributed Approach for Detecting and Mitigating DDoS Attacks on White-Boxes 15
Pablo Armingol Robles, Antonio Agustín Pastor Perales, Juan Carlos Caja Díaz

Detecting Malicious Websites by Using Deep Q-Networks 23
Khanh Nguyen, Younghee Park

The Study of Feature Engineering in Machine Learning and Deep Learning for Network Intrusion Detection Systems 33
Steven Ning, Khanh Nguyen, Sohini Bagchi, Younghee Park

Smart DC Microgrid Architectures and Its Cyber Security Challenges: An Overview 38
Jetwadee Phanthanachai, Manoj Tripathy, Balakrishana Pamulaparthy

Unmasking the Vulnerabilities of Deep Learning Models: A Multi-Dimensional Analysis of Adversarial Attacks and Defenses 46
Firuz Juraev, Mohammed Abuhamad, Eric Chan-Tin, George K. Thiruvathukal, Tamer Abuhmed

The Impact of Model Variations on the Robustness of Deep Learning Models in Adversarial Settings 54
Firuz Juraev, Mohammed Abuhamad, Simon S. Woo, George K Thiruvathukal, Tamer Abuhmed

A Gaze-Based Analysis of Human Detection of Email Phishing 61
Francesco Pietrantonio, Alessio Botta, Stefania Zinno, Giorgio Ventre, Luigi Gallo, Laura Mancuso, Roberta Presta

Multimodal Sentiment Analysis: Perceived Vs Induced Sentiments 69
Aditi Aggrawal, Deepika Varshney

Attack Group Analysis and Identification Based on Heterogeneous Graph 76
Taehyun Han, Sangyeon Hwang, Tae-Jin Lee

Exploring Scalable Bayesian Networks for Identification of Zero-Day Attack Paths 82
Ravi Nitinkumar Patel, Xiaomei Zhang, Xiaoyan Sun, Jun Dai

Quantum Implementation and Analysis of ARIA 90
Yujin Oh, Kyungbae Jang, Yujin Yang, Hwajeong Seo

Depth Optimized Quantum Circuits for HIGHT and LEA 97
Kyungbae Jang, Yujin Oh, Minwoo Lee, Dukyoung Kim, Hwajeong Seo

PoE: A Domain-Specific Language for Exploitation 103
Jung Hyun Kim, Steve Gustaman, Sang Kil Cha

The Threat of Password Guessing Attacks Exploiting Linguistic Characteristics: A Case Study on the Korean Domains 109
Minah Chae, Wongeun Shin, Sangyun Jung, Jihun Yeom, Dongho Jeon, Heeseok Kim

Simplified Quantum Circuit Implementation for ASCON Security Analysis Against Grover's Algorithm 113
Jinseob Oh, Chanho Choi, Dooho Choi

Human-To-Device (H2D) Authentication Using Biometrics 116
Mohammadreza Hosseinzadehketilateh, Sara Tehranipoor, Nima Karimian

Combating Deepfakes: A Novel Hybrid Hardware-Software Approach 119
Kamrul Hasan, Nima Karimian, Sara Tehranipoor

5G Remote eSIM Provisioning: Blockchain-Based Public Key Delivery 121
Rono Cheruiyot, Sourav Purification, Simeon Wuthier, Sang-Yoon Chang

Analyzing the Container Security Threat on the 5G Core Network 124
Jihyeon Song, Kyungmin Park, Cheolhee Park, Jonghyun Kim, Ikkyun Kim

ProtectNIC: SmartNIC-Based Ransomware Detection 127
Anson Xu, Arnav Choudhury, Eason Liu, Sean Choi

Graph Neural Networks for Network Intrusion Detection: An IP Behavioral Analysis Perspective 130
Seon Woo Lee, Ju Young Lee, Tae Jin Lee

Toward Post-Quantum Digital Certificate for eSIM 133
Qaiser Khan, Sourav Purification, Rono Cheruiyot, Jinoh Kim, Jonghyun Kim, Sang-Yoon Chang

Wireless Link Routing to Secure Against Fake Base Station in 5G 136
Sourav Purification, Kyungmin Park, Jinoh Kim, Jonghyun Kim, Sang-Yoon Chang

Exploring Reinforcement Learning to Aid Tor Latency Performance 139
Kelei Zhang, Sang-Yoon Chang

Hop-Count Authentication with Moving Keys for Mobile Ad Hoc Networks 142
Seonho Choi

Side-Channel Protected PIPO Implementation in Hardware 145
Jaeseung Han, Yeon-Jae Kim, Dong-Guk Han

Author Index