

2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs 2023)

**Bogor, Indonesia
22-24 August 2023**



**IEEE Catalog Number: CFP23FZ5-POD
ISBN: 979-8-3503-3944-4**

**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:	CFP23FZ5-POD
ISBN (Print-On-Demand):	979-8-3503-3944-4
ISBN (Online):	979-8-3503-3943-7

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

Words of Welcoming	i
Committees	iii
Program Schedule	v

Tailoring e-Government’s ICT Readiness for Business Continuity based on Cyber-Risk Approach	1
<i>Saffana Tistiyani, Obrina Briliyant and Nanang Trianto</i>	
PDFfalse: Evasive Malicious PDF Machine Learning Classifier	9
<i>Gusti Agung Ngurah Gde K.T.D and Girinoto</i>	
Performance and Security Comparison of Json Web Tokens (JWT) and Platform Agnostic Security Tokens (PASETO) on RESTful APIs	15
<i>Adiva Fiqri Nugraha, Herman Kabetta, I Komang Setia Buana and R Budiarto Hadiprakoso</i>	
Comprehensive Analysis and Remediation of Insecure Direct Object References (IDOR) Vulnerabilities in Android APIs	23
<i>Semi Yulianto, Roni Reza Abdullah and Benfano Soewito</i>	
Comparative Analysis of Attack Behavior Patterns in Petya, CryptInfinite, and Locky Ransomware Using Hybrid Analysis	29
<i>Arga Yuda Prasetya, Khirsa Inayatul Aini and Charles Lim</i>	
Matrix NTRU Cryptosystem over Integral Domain	35
<i>Indah Emilia Wijayanti, Uha Isnaini, Anny Kartika Sari, Saifullah Ali and Novian Deny Cahyo Aji</i>	
Secure Self Payment and Monitoring Service Laundry using RFID with SHA-3 and AES 128	41
<i>Erfandra Ramadhan, Anita Rizkiana, Patar Wiyardhana and Dion Ogi</i>	
Performance Test of Hash Functions in Proof of Work Schemes in Blockchain	47
<i>Luthfi Hakim Panuntun, Bety Hayat Susanti and Sri Rosdiana</i>	
Mobile Forensic Imaging Prototype with Data Integrity	53
<i>M Jaya Hadi Kusuma, Rizka Khairunnisa and Fetty Amelia</i>	
Automating News Tweet Writing Based on Indonesia Language Using NLG Approach	59
<i>Christina Christina, Indra Aulia and Sarah Purnamawati</i>	
Exploration of Malicious Applications on Digital Invitations with Static Analysis Method Using ImmuniWeb	66
<i>Ilham Dwi Harjanto, Irman Yunal Wirdani, Charles Lim and Mareta W. Ardyani</i>	
Implementation of ChaCha20 Algorithm with Elliptic-Curve-Diffie-Hellman in Server Room Monitoring System to Prevent MITM and Reused Key Attack	71
<i>Danang Enggar, Habib Al Fitrah, Malika Ayunasari and Dion Ogi</i>	
Implementing CRYSTALS Kyber and Dilithium in Intel SGX Secure Enclaves	77
<i>Nabila Pratiwi, M. Rafli Firmansyah and Martianus Frederic Ezerman</i>	

Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government	82
<i>Eko Yon Handri, Prasetyo Adi Wibowo Putro and Dana Indra Sensuse</i>	
Intrusive Detection Techniques Utilizing Machine Learning, Deep Learning, and Anomaly-based Approaches	88
<i>Mayur Rele and Dipti Patil</i>	
On a Small Class of Binary Modified de Bruijn Sequences of Maximal Linear Span	94
<i>Musthofa Musthofa, Indah Wijayanti, Diah Palupi and Martianus Ezerman</i>	
Image-Based Malware Classification: A Systematic Literature Review	99
<i>Yudhistira Yudhistira, Dimas Wahyu Utomo and Charles Lim</i>	
Integral Distinguisher on 5 Rounds SLIM Algorithm	104
<i>Kamila Amalia and Santi Indarjani</i>	
Investigating the Impact on Data Recovery in Computer Forensics	109
<i>Semi Yulianto and Benfano Soewito</i>	
Feature Extraction Methods and Classification for Malware Incident News	115
<i>Gugum Gumilar, Eka Budiarto, Maulahikmah Galinium and Charles Lim</i>	
Implementation of N-Gram Method for Automating News Ticker Generation Based on Indonesian Language	121
<i>Felipe Felipe, Indra Aulia and Erna Budhiarti Nababan</i>	
Optical Fiber Network Design and Analysis of Mass Rapid Transit Phase Three for Communication Link	127
<i>Felix Yaman Kusuma, Rifqi Annas Albasyahri, Hanna Putri Shabira, Ryan Daniel A. Sibagariang, Nolland Zidane Tamar Dandika, Salma Azra Fatimah, Salman Elfarizi and Catur Apriono</i>	
Communication Efficient on Symmetric and Asymmetric Encrypted Anonymous Federated Learning	133
<i>Muhammad Senoyodha Brennaf, Po Yang and Vitaveska Lanfranchi</i>	
Enhancing Cyber Attribution through Behavior Similarity Detection on Linux Shell Honeybots with ATT&CK Framework	139
<i>Kevin Hobert, Charles Lim and Eka Budiarto</i>	
Text-based File Security with Signcrypton Using AAβ and DSA Algorithms	145
<i>Lathifah Ain, Mohammad Budiman and Maya Lydia</i>	
The Meet-in-The-Middle Attack on The Matrix NTRU Cryptosystem	149
<i>Khoirun Nisa, Indah Emilia Wijayanti and Khoirun Nisa</i>	
Analysis of SYN Flood Attack Detection on Web-Based Services Using Round Trip Time (RTT) Calculation	154
<i>Nugroho Adi Wibowo, Dessy Ariami and Charles Lim</i>	
Cryptanalysis on Polynomial Congruence-Based Public Key with Chinese Remainder Theorem	159
<i>Ikhwanul Hakim Masri and Bety Hayat Susanti</i>	
Comparative Study of Open-Source Firewall	165
<i>Jeckson Sidabutar, Dimas Febriyan Priambodo, Noni Fauziah Septianty, Kevin Yehezkiel Gurning and Fresly Juliarta</i>	

A Linear Cryptanalysis on Simplified Kuznyechik 2	173
<i>M. Ikhsan Mubarok and Santi Indarjani</i>	
Unveiling Attack Patterns: A Study of Adversary Behavior from Honeypot Data	178
<i>Dimas Subhan and Charles Lim</i>	
A Novel Digital Forensic Readiness (DFR) Framework for e-Government	184
<i>Hernowo Adi Nugroho, Obrina Briliyant and Septia Sunaringtyas</i>	
Optical Fiber Network Submarine Design in Timor Leste Based on the Palapa Ring Project	190
<i>Fidelio Soares, Habib Nurseha Anggradinata and Catur Apriono</i>	
A Modified Zero-Knowledge Scheme from Bilinear Pairing for Securing Multiple Secret Values	195
<i>Annisa Handayani, Sa'Aadah Carita and Nia Yulianti</i>	
Detection of DDoS on SDN Data Plane Through Mirror Traffic	199
<i>I Made Adhiarta Wikantayasa and Tohari Ahmad</i>	
Redline Stealer Malware Analysis with Surface, Runtime, and Static Code Methods	205
<i>Fahmi Ramadan and Ira Rosianal Hikmah</i>	
Algebraic Attack on 2-Round SMALLPRESENT-[2] Algorithm	212
<i>Tsamara Khadijah Silim, Muhammad Faturrohman Sugiyarto, Nadia Paramita Retno Adianti and Santi Indarjani</i>	
Digital Forensic Analysis of Online Dating Applications on Android Using the Digital Forensic Research Workshop 2001 Investigation Model	218
<i>Nafiz Feizal Mahendra and Rizka Khairunnisa</i>	
Implementation of AES-256 Algorithm for Secure Data Transmission in LoRa-Based Forest Fire Monitoring System	224
<i>Ariska Allamanda, Bella Wulandari, Muhamad Nadhif and Dion Ogi</i>	
A Proposed Architecture for The Indonesia's National Blockchain	230
<i>Dea Saka Kurnia Putra and Amiruddin</i>	
Verifiable Timed Commitments for Fair Sealed-bid Auctions	236
<i>Duygu Özden and Oğuz Yayla</i>	
Analysis and Improvement of JPEG Compression Performance with Discrete Cosine Transform and Convolution Gaussian Filtering	246
<i>Ronald Suryadi Purba, Tulus and Saib Suwilo</i>	
Comparison of Transfer Learning Performance in Image-Based Malware File Classification on the Dumpware10 Dataset	252
<i>Febri Putra Sandhya Prawiranata and Raden Budiarto Hadiprakoso</i>	
Comparative Analysis of Recovery Tools for Digital Forensic Evidence Using NIST Framework 800-101 R1	258
<i>Muhammad Surya, Jeckson Sidabutar and Nurul Qomariasih</i>	
Modification of LAKA Protocol Using Fuzzy Verifier and Honeywords	263
<i>Fendy Heryanto, Sepha Siswantyo and Almalika Setya Widyanti</i>	
Investigating Multiple Malware as a Service (MaaS): Analysis and Prevention Techniques	270
<i>Grace Friscilla Margaretha Karo-Karo, Muhammad Sofyan Arif Harumnanda and Charles Lim</i>	
Knowledge Graphs for Cybersecurity: A Framework for Honeypot Data Analysis	275
<i>Yevonnael Andrew, Charles Lim and Eka Budiarto</i>	

InnerCheck: A New Breakthrough for Early Detection of Mental Health	281
<i>Dika Agustian Akbar, Dzakwan Al Dzaky Bewasana, Ahmad Zainudin Mahfud and Tiyas Yulita</i>	
Comparative Analysis of Deep Learning Models for Web Defacement Detection Based on Textual Context	287
<i>Shakira Putri Ayunda, Raden Budiarto Hadiprakoso, Nurul Qomariasih and Herman Kabetta</i>	
Comparison of Meet-in-the-middle Attacks On 2-DES and 2-AES with Four Scenarios	292
<i>Sandy Tri Kurnia, Yeni Farida and Santi Indarjani</i>	
A New Boundary of Minimum Private Key on Wiener Attack Against RSA Algorithm	297
<i>Muhammad Dandi Pradana, Salsa Sabila Baladina, Annisa Dini Handayani and Sa'Aadah Sajjana Carita</i>	
Cyber Threat Hunting to Detect Unknown Threats in the Enterprise Network	303
<i>Arssy Hasyir Nursidiq and Charles Lim</i>	
Deep Learning for Android Malware Detection and Classification Using Hybrid-Based Analysis: A Comparative Study	309
<i>Arga Prayoga, Raden Budiarto Hadiprakoso, Girinoto and Ray Novita Yasa</i>	
A Low-Cost Disk Imaging Device Using Raspberry Pi 4 for Digital Forensics	314
<i>Catur Adi Nugroho and Amiruddin</i>	
Cybersecurity Risk Assessment for Beninese power grid SCADA system	320
<i>Aurélie Kpoze, Jules Degila, Samuel Fosso Wamba, Pélagie Houngue, Henoc Soude and Arnaud Ahouandjinou</i>	
Comparative Analysis of Forensic for Whatsapp Desktop on Mac OS and Windows Using IDFIF V2	327
<i>Faris Firana Febrian and Jeckson Sidabutar</i>	
Cyber Risk Management Planning Based NIST CSF ISO 27005 NIST SP 800 53	332
<i>Ellisa Hani Nur Safitri and Herman Kabetta</i>	
Author Index	339