IFERP®
Explore Your Research Journey...

CALL FOR BOOK CHAPTERS 2024

Technoarete® Publishing
Integrating Researchers to Incubate Innovation

Artificial Intelligence Approaches for Cyber Security and Digital Forensics

(with ISBN Number : 978-93-92104-03-9)

After Publication the Book Chapter will be submitted to WoS and SCOPUS for Indexing

Abstract Submission Deadline	Abstract Acceptance Notification	Full Chapter Submission Deadline	Acceptance / Revision Notification	Revised Chapter Submission	Acceptance / Rejection Notification	Camera Ready Paper Submission
29 February 2024	15 March 2024	05 April 2024	01 May 2024	20 May 2024	10 June 2024	30 June 2024

Scope of the Book

Recent days record steep rise in the adoption of artificial intelligence techniques for cyber security and digital forensics application global cost of data breach report to be around $3.8milloin considering such huge figure of financial loss, applying artificial intelligence techniques could simplify processing of massive volumes of data, maintaining error free cyber security, identifying the micro level threats in cyber haystacks, improving cyber threats detection and automation, improving the threat detection and response time, tackling advanced hacking techniques, securing authentication and many more. This book aims to cover a wide range of areas and application in cyber security and digital forensics where artificial intelligence mechanisms and techniques play a major role.

Editors

Dr.S.Balamurugan
Ph.D., D.Sc., SMIEEE
ACM Distinguished Speaker,
Director - Albert Einstein Engineering and Research Labs (AEER Labs)
Vice Chairman - Renewable Energy Society of India (RESI), India

Dr.Ramasamy V
Ph.D.,
Assoc. Prof., Department of CSE,
Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology (Deemed to be University),
Chennai, Tamil Nadu, India

Mr.Fredrik Hofflander
Chief Technology Officer at eghed
Co-Founder of delori
Chair of the Board, AI Center Greater Gothenburg
Sweden

Recommended Topics

- Deep Fakes
- Spear Phishing Emails
- Cloud Forensics
- Cyber Kill Chain
- Hard Disk Forensics
- Digital Forensic Tools
- Cyber Stalking
- Email Bombing Detection
- Cyber Attacks and Risk Management
- Spam Filtering using Artificial Intelligence
- Biometric Fingerprint Recognition
- Generative Deep Learning for Digital Forensics
- Machine Learning Techniques for Handling Malware Attacks
- Artificial Intelligence Techniques to Detect Malicious Mail
- Artificial Intelligence for Automatic Detection of Ransomware
- Secure Network Packet Classifications using Machine Learning
- Privacy Preserving Social Network Data Publishing
- Credit Card Fraud Detection using Artificial Intelligence Techniques
- Cryptocurrencies Price Prediction using Machine Learning

*Original Contributions from the authors are invited on the following topics (Not limited to)

Important Points to Consider

- Plagiarism check should be done using Turnitin.
- Plagiarism must not exceed 10%
- Full Chapter will be 20 to 25 Pages.
- Published with ISBN Number
- DoI for Book
- Individual DoI for every accepted Chapter
- The book will be submitted to SCOPUS and WoS for Indexing after publication.
- E-book Access from Publishers websites, Amazon Kindle & Flipkart
- Accepted Chapters authors should pay a publication fee of,

₹1500 INDIA (INR)

$25 ABROAD (USD)

Guidelines for Book Chapter contributors can be Located at
www.iferp.in/book-chapter/submission-guidelines.pdf

All Submissions and Queries must be Directed to the Following Email
editorbook@technoarete.org