Call for Book Chapters

Book Title: Privacy, Security and Forensics in The Internet of Things (IoT)

Publisher: Springer

Synopsis

Despite its numerous beneficial use, the Internet of Things (IoT) devices simultaneously present numerous challenges including those related to privacy, security and data breaches, or those pertaining to ethical, legal and jurisdictional matters. These issues are further compounded by the technical challenges resulting from the heterogeneous nature of these devices that have a broad range of proprietary hardware and software that often use different data formats, network or communication protocols, and physical interfaces. Similar challenges posed by the IoT devices concern the fact they access and use large quantities of private data that could be sensitive to individuals or organisations. This data can be rapidly transferred from one device to several other connected devices, creating a wider security attack surface. The spread of this data across multiple devices and platforms combined with anti-forensic methods and jurisdiction and service level agreements (SLA) all further aggravate technical, privacy, security and legal challenges presented by the IoT. Considering these challenges, we welcome book chapter contributions of 7,000 to 10,000 words centred (but not exclusively) on the following themes:

1. Cyber Threat Prediction and Modelling
2. Securing the IoT Devices in Smart Homes against Ransomware Attacks
3. Reinforcing the Industrial Internet of Things Security Using Digital Twin Simulations
4. Distributed Chain of Custody and Blockchain
5. Digital Forensic Frameworks for Cryptocurrency Investigations
6. Training Future Cryptocurrency Investigators: Practitioner Led Training
7. A Comprehensive Analysis of European Cyberlaws: Challenges, Limits and Recommendations
8. Legal Considerations and Ethics of AI in the IoT and Smart Cities
9. AI-Enabled IoT Forensics within the Confines of the ISO 17025 and Forensic Science
10. Cyber Abuse and Investigatory Models in Smart Societies
11. Unmanned Aerial Vehicle Forensics
12. The Malicious Use of AI in the IoT Environments
13. An AI-Based Approach for Forensically-Sound Exhibit Handling and Documentation
14. Data Acquisition and Analysis of Vehicle Infotainment and Telematics Systems Data
15. AI-Enabled Models for Forensic Acquisition and Analysis of Digital Objects in Smart Cities
16. A Machine Learning-Assisted Triage Approach for Automated Classification of Smart Devices
17. Digital Twinning in Cyber Security Testing and Resilience
18. Human Factors in the IoT Security to Improve Perceptions of Security and Privacy Concerning IoT Devices
19. Smart City Security Designs, Solutions and Services to Improve Risk Assessment and Decision Making
20. Usable Security, Cyber Security Awareness, and Cyber Situational Awareness

Important Dates

- Full Chapter Submission: **May 01, 2021**
- Acceptance/Rejection Notification: **May 15, 2021**
- Revised Version Submission: **June 07, 2021**
- Acceptance/Rejection Notifications: **June 10, 2021**
- Camera Ready Submission: **June 20, 2021**

Important Notes for Prospective Authors

Submitted papers must not have been previously published nor be currently under consideration for publication elsewhere. Conference papers may only be submitted if the paper has been completely re-written and the author has cleared any necessary permission with the copyright owner. All chapters will undergo a peer review process by 3 or more reviewers. There are no submission or acceptance fees for manuscripts submitted to the publication of this book.

Manuscript Preparation

Full chapter length must range between 7,000 to 10,000 words and contain a minimum of 5 key words. Chapter submissions must be prepared in accordance with the publisher's **submission guidelines** for manuscripts. Only electronic submissions in PDF format will be considered.

Submission Procedure

All manuscripts must be submitted through EasyChair using the following submission link **IoTSCPSF-2021.**

Book Editors

Dr. Reza Montasari
Hillary Rodham Clinton School of Law, Swansea University
Email: Reza.Montasari@Swansea.ac.uk.

Dr. Rachel Bolton-King
School of Law, Policing and Forensics, Staffordshire University
Email: r.bolton-king@staffs.ac.uk.

Dr. Fiona Carrol
School of Technologies, Cardiff Metropolitan University
Email: fcarroll@cardiffmet.ac.uk.

Dr. Ian Mitchell
School of Science and Technology, Middlesex University
Email: I.Mitchell@mdx.ac.uk.

Mrs. Sukhvinder Hara
School of Science and Technology, Middlesex University
Email: S.Hara@mdx.ac.uk.

Email Enquiries

Please address any queries to Reza Montasari at **Reza.Montasari@Swansea.ac.uk.**