Taylor & Francis Group

Editors

Dr. Kayhan Zrar Ghafoor,
Salahaddin University-Erbil, Kurdistan, Iraq
Email: kayhan@ieee.org

Dr. Kevin Curran
Ulster University, UK
Email: kj.curran@ulster.ac.uk

Dr. Linghe Kong
Shanghai Jiao Tong University, China
Email:linghe.kong@sjtu.edu.cn

Dr. Ali Safa Sadiq
University of Wolverhampton, UK
Email:ali.Sadiq@wlv.ac.uk

Important dates

Chapter Proposal Submission:
October 1, 2019
Chapter Proposal Notification:
November 1, 2019
Full Chapter Submission:
January 15, 2020
Review Results Returned:
March 1, 2020

Final Chapter Submission:
May 15, 2020

Call for Book Chapters

"Artificial Intelligence Applications for A Smart Cyber Ecosystem: Smart Cities, Cybersecurity and IoT"

.

Call for Book Chapters:

Artificial Intelligence Applications for A Smart Cyber Ecosystem: Smart Cities, Cybersecurity and IoT

To be published by Taylor & Francis Group, USA

Over the last few years we have witnessed a rapid growth in Internet of Things (IoT) that provides ubiquitous connectivity between physical components and cyber space. Recent advances in hardware, software, networking technologies have fueled the deployment of IoT technologies. Additionally, smart cities have also become a promising field of study that encompasses distributed large scale sensing, data acquisition, information processing and heterogeneous networking. Smart cities aim to improve the quality of life of citizens in several areas such as energy usage, healthcare, environment, water and transportation. However, smart cities will not only impact the private information of citizens but will also have a direct effect on city services that are directly related to the daily life of citizens. The connectivity of billions of IoT devices opens up many security vulnerabilities and threats that must be detected and mitigated. There is a significant interest to enable Artificial Intelligence (AI) techniques- that incorporates meta-heuristics, machine learning and optimization algorithms- for intelligent IoT communications and networking management, studying significant characteristics of IoT networks and offering intelligent Cybersecurity solutions in smart cities. Besides, machine learning algorithms and big data techniques open up indispensable opportunities to further analyse the characteristics of IoT networks.

AI is evolved as an important tool and an attractive research topic that constitutes a promising solution for IoT network optimization, intelligent attack analysis and detection, and providing quality of service (QoS) to deployed smart cities networks. Thus, it is becoming necessary to develop an intelligent techniques powered by AI to enable smart decision, adaptation and modeling various technical problems in next-generation massively connected IoT devices.

This book aims to provide latest research developments and results in the domain of AI techniques for smart cyber ecosystem. It presents a holistic insight into AI-enabled theoretic approaches and methodology in IoT networking, security analytics using AI tools, and network automation, which ultimately enable intelligent cyber space. This book will be a valuable resource for students, researchers, engineers, policy makers working in various areas related to cybersecurity and privacy for Smart cities.

Topics of interest include, but are not limited to, the following:

- AI: Evolution and fundamental concepts
- Smart City: Evolution and fundamental concepts
- Cybersecurity and privacy fundamentals
- Networking and security architectures for Smart City applications
- AI-based Cyberattack analyses and attack patterns in Smart Cities
- Intelligent Cybersecurity as a Service
- AI enabled Big data analytics for cybersecurity in Smart Cities
- AI enabled Cybersecurity of critical infrastructures for Smart Cities
- IoT resource allocation & management using AI Techniques
- AI enabled IoT communication defects diagnosis
- Deep learning approaches for indoor localization of IoT devices in smart cites
- AI technologies for network mobility management
- Future AI algorithm challenges for smart cyber ecosystem

Submission Guidelines

Prospective authors are required to submit your chapter to kayhan@ieee.org. All submitted manuscripts will be passing through the rigorous reviewing process for possible publication. All book chapters should be prepared in Latex/MS Word format according to Taylor & Francis Group's guidelines for manuscript preparation.