Guest Editorial Preface

Special Issue on Recent Advances in Cyber Security and Privacy for Cloud-of-Things

Yassine Maleh, Hassan 1st University, Casablanca, Morocco
Ghita Mezzour, International University of Rabat, Rabat, Morocco
Marinella Petrocchi, Institute for Informatics and Telematics IIT, Pisa, Italy
Abdelkrim Haqiq, Hassan 1st University, Casablanca, Morocco

In recent years, Cloud of Things CoT has emerged as a revolutionary paradigm that enables intelligent and self-configuring (smart) IoT devices and sensors to be connected with the cloud through the internet. The Cloud of thing paradigm can stimulate the development of innovative and novel applications to various areas such as smart cities, smart homes, smart grids, smart agriculture, smart transportation, smart healthcare, etc. In the Cloud of Things system field, security and privacy threats have been extensively studied and received considerable attention in recent years, as witnessed by the number of related publications. In the context of these trends, the forthcoming special issue on recent advances on cyber security and privacy for Cloud-of-Things will address significant issues in the field. Topics covered include issues of personal information and identity crime for cloud of thing, intellectual property-related issues in cyberspace, computer forensic investigation in cloud of things, etc.

The main goal of this special issue is to encourage both researchers and practitioners to share and exchange their experiences and recent studies with a particular emphasis on interdisciplinary approaches and novel techniques to increase the security posture of Cloud of Things devices (smart sensors, 6lowpan, M2M, IoT, etc.). The overall objectives are:

- To improve the awareness of readers about cyber Security and Privacy for Cloud-of-Things;
- To analyze and present the state-of-the-art of the cyber Security and privacy for Cloud-of-Things and Edge Computing and related technologies and methodologies;
- To highlight and discuss the recent development and emerging trends related to cyber Security and privacy for Cloud-of-Things;
- To propose new models, practical solutions and technological advances related to cyber Security and privacy for Cloud-of-Things;
- Discusses new cyber Security and privacy models, prototypes and protocols for the Cloud of Things environment.

A special thank you to all the authors who submitted their articles to this special issue and a special thank you to all the authors whose four articles are published in this special issue. I hope that contributors will have greater visibility and impact through this research publication.

The special issue is organized into five articles. A brief description of each of the papers follows.

Article 1 by Junaid Latief Shah, et al. entitled “CloudIoT - Towards seamless and secure integration of cloud computing with Internet of Things,” presented a survey on the integration components of

CloudIoT and presented diverse applications including driving factors for CloudIoT integration. The paper also identified security vulnerabilities implied by integration of Cloud and IoT and outlines some suggested measures to mitigate the challenge. Finally; the paper proposed some open issues and challenges providing potential directions for future research in this area.

Article 2 by Md. Muzakkir Hussain et al. entitled "Big data analytics platforms for electric vehicle integration in transport oriented smart cities computing platforms for platforms for electric vehicle integration in smart cities," considered the case of Electric Vehicle (EV) to Smart Grid (SG) integration. The EVs are key players for Transport Oriented Smart Cities (TOSC) as they help cities to become greener by reducing emissions and carbon footprint. The authors analyzed different use-cases in EV to SG integration to show the scope of Big Data Analytics (BDA) platforms towards successful EV rollout. Then, the paper presented two computing platforms, distributed cloud computing, and edge computing, and discussed their features for supporting BDA activities in EV integration.

Article 3 by S.J. Sheela et al. entitled, "Secured transmission of clinical signals using hyperchaotic DNA confusion and diffusion transform," introduced a new cryptosystem for clinical signals such as electrocardiograms (ECG) and electroencephalograms (EEG) based on hyperchaotic DNA confusion and diffusion transform (HC-DNA-CDT). The algorithm used hyperchaotic system with cubic nonlinearity and deoxyribonucleic acid (DNA) encoding rules.

Article 4 by Vinayakumar et al. entitled "A comparative analysis of deep learning approaches for network intrusion detection systems (N-IDSs)," focused to apply deep learning techniques to network intrusion detection (N-IDS) with the aim to enhance the performance in classifying the network connections.

Article 5 by El Makkaoui et al. entitled "Cloud-ElGamal and Fast Cloud-RSA homomorphic schemes for protecting data confidentiality in cloud computing", presented the Homomorphic Encryption schemes for cloud computing and analyzed their security, and implemented the schemes, compared and discussed their efficiency.

We hope this special issue would kindle interest of several researchers in the field of cyber security and privacy for Cloud-of-Things.

Yassine Maleh
Ghita Mezzour
Marinella Petrocchi
Abdelkrim Haqiq
Guest Editors
IJDCF