Annals of Emerging Technologies in Computing (AETiC)

Print ISSN: 2516-0281 Online ISSN: 2516-029X
Volume #4 Issue #5 December 20, 2020

Editorial

Dear Reader,

This special issue, "Industrial Security for Smart Environments" of Annals of Emerging Technologies in Computing (AETiC), comprises 5 papers that are the latest advances in basic and applied research in the field of smart environments industrial security. Smart environments research has grown to be one of the most influential academic and industry fields that can strongly contribute to industrial applications. However, the security issue still a major concern for those applications.

In this special issue, we invited submissions exploring the latest advances in the field of smart industrial environments. It originally attracted 10 submissions, among which 5 regular papers were selected for inclusion in the special issue after a rigorous review process. The accepted papers illustrate the highly innovative and informative venue for essential and advanced scientific and engineering research in industrial security for smart environments.

Alam *et al.* introduced a review paper on the distributed intelligence at the edge of the Internet of Things (IoT) networks. The paper reviewed the state-of-the-art of distributed technologies and the distributed intelligence concepts and their usage in IoT. Besides, it classifies the IoT different applications and related challenges, including security.

Omar Dib and Khalifa Toumi introduced the architectures, challenges, solutions, and future directions for decentralized identity systems. The paper focuses mainly on the decentralized identity systems based on blockchain describing their architectures, components, lifecycle, and workflow. It also introduces the Self Sovereign Identity (SSI) paradigm as a new Identity Management Systems (IMS) based on blockchain. SSI has quantitatively evaluated the security levels of SSI solutions.

Dhirani and Newe reviewed Cloud Service Level Agreements (SLA) for Industry 4.0. The paper discusses the details of SLA and its implementation on the key player vendors such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and International Business Machines Clouds (IBM Cloud). Besides, the paper tries to bridge the SLA gaps between Industrial cloud tenants and vendors and developing insights on cloud QoS issues that otherwise stay disguised/unknown to the non-expert.

Ramadan and Yadav proposed a Hybrid Intrusion Detection System (IDS) to detect Internet of Things (IoT) Network Attacks. The paper tries to reduce the required detection time and

feature selection as well as the classification. The paper's first stage, the feature selection process, is accomplished using the Enhanced Shuffled Frog Leaping (ESFL) algorithm, and the selected features are classified using Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN) algorithm.

Haque *et al.* proposed an Integer Linear Programming (ILP) model to optimize the DDoS Attack of Software-Defined Networking (SDN) security issue by placing a powerful smart backup controller. The paper proposes a single or multiple smart backup controller placement to support several ordinary victim controllers. This saves the cost of multiple ordinary controllers by sharing a link, maximum new flows per second of controller and port, etc.

Finally,
Rabie A. Ramadan (Special Issue Editor),
On behalf of the Editorial Board,
Annals of Emerging Technologies in Computing (AETiC).