IEEE Transactions on Industrial Informatics

# Guest editorial: AI-enabled threat intelligence and hunting microservices for distributed industrial IoT system

Nour Moustafa, Guest Editor
School of Engineering and Information Technology, University of New South Wales (UNSW Canberra), Campbell, ACT 2612, Australia

Kim-Kwang Raymond Choo, Guest Editor
Department of Information Systems and Cyber Security
University of Texas at San Antonio, San Antonio, TX 78249 USA

Adnan M. Abu-Mahfouz, Guest Editor
Council for Scientific and Industrial Research and Department of Electrical and Electronic Engineering Science, University of Johannesburg, Pretoria 0002, South Africa

https://ieeexplore.ieee.org/document/9536391

**Abstract**

Industrial Internet of Things (IIoT) systems are increasingly found in settings such as factories, smart cities/nations, and healthcare institutions. These systems facilitate the interconnection of automation and data analytics across different industrial technologies, such as cyber-physical systems, Internet of Things (IoT), and cloud and edge computing devices and systems. However, IIoT systems also generate significant volume of data, which can incur significant overheads in processing such data at cloud centers [A1]. Existing IIoT systems may be developed as monolithic architecture, where such a system is deployed as a single solution. In this architectural design, few programming languages can be used to create a single application or process composed of several classes, methods, and packages, in which the entire application is executed in one server irrespective of the application requirements.