Guest Editorial: AI-Enabled Threat Intelligence and Hunting Microservices for Distributed Industrial IoT System

I. Introduction

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.

This monolithic design of applications is module independent, has a uniform standard, is simple to develop and test, and scales horizontally. However, it has poor scalability as any overload in its functions could cause a bottleneck of execution, and any change in one function would affect other dependent functions. Additionally, this design increases the complexity of redeployment and maintenance, causing difficulty in solving heterogeneity-related challenges. To overcome the challenges associated with monolithic design, the potential of microservice architecture has been explored in [A2], where a single solution or application is divided into small manageable components (e.g., services). Every single microservice performs a single function and is independent of others. In addition, any programming language can be used to realize each provided microservice. In contrast to monolithic architecture, microservice reduces the complexity of redeploying and maintenance because the microservices are independent and can easily be modified and changed. Moreover, it supports many technology stacks and fault tolerance which, in turn, makes it more scalable.

For designing the most appropriate architecture for distributed IIoT systems, modular properties of microservices should be considered to enhance the performances of deploying applications. In a distributed IoT system, the instances of the microservices are scaled based on the load, which changes the number of microservices and their locations dynamically. Several considerations need to be taken when deploying microservices including service discovery, interservice communication, data integrity, security, monitoring and health check, and quality assurance. The heterogeneity of IIoT data creates different challenges for existing data processing techniques when they handle heterogeneous data sources in IIoT networks. Therefore, new techniques are needed to harness the security of data and enhance the processing of heterogeneous data sources.

Artificial intelligence (AI) technology assists in inferring valuable knowledge from data generated by a device or human; thus, implementing AI through microservices cab enhance the process of learning large-scale and heterogeneous data sources [A3]. AI-enabled microservices can be leveraged within IIoT systems for supporting intelligent services and enable the implementation of modular security techniques. There are microservice solutions, including Docker Swarm, OpenStack Magnum, and Kubernetes, which decompose applications and deploy a set of services to allow the execution of AI-enabled applications. Microservice orchestration techniques have been independently used in the cloud, edge, and IoT/IIoT systems. But, there is no standard architecture, which facilitates the implementation of AI-enabled threat intelligence and hunting microservices in distributed IIoT networks. Existing service orchestration and microservice approaches, methods, and frameworks have challenges related to the flexibility, security, and privacy of distributed IIoT systems, which do not enable the automation of the service orchestration management in a federated IIoT environment.

This Special Section on "AI-Enabled Threat Intelligence and Hunting Microservices for Distributed Industrial IoT System" highlights the main research challenges in the AI-based security and privacy microservices for IIoT systems. Of the 39 submissions, seven articles were eventually accepted after undergoing several rounds of rigorous peer reviews (i.e., acceptance rate of 17.95%). We will now introduce these seven articles in Sections II–V.

II. Threat Hunting and Intelligence

Threat hunting and intelligence methods have become attractive areas of research for understating cyber-attack behaviors and how they occur. The development of these methods depends on

Digital Object Identifier 10.1109/TII.2021.3111028

utilizing and modeling attack activities from systems, including intrusion-detection systems [A4], security information and event management, as well as security operation center. The intelligence of threat detection has become a big challenge that should effectively deal with large-scale and heterogeneous data sources of IIoT networks.

In [A5], suggested a novel federated deep learning model (Fed-TH) for addressing the challenge of threat detection and hunting cyber-attacks via extracting the temporal and spatial representations of network data. Then, a container-based industrial edge computing framework was designed to implement the proposed Fed-TH model as a threat-hunting microservice on edge servers. To address the latency problem, an exploratory microservice placement method was also suggested to allow high performance of deploying the proposed model through microservices.

III. Blockchain

Blockchain has been coined to offer transparent and integrity characteristics for various IIoT applications. One of the key limitations of IIoT applications is privacy leakage and insufficient model accuracy. To address this limitation, Youliang *et al.* [A6] presented a blockchain-based machine learning framework for edge services in IIoT systems. To be specific, a smart contract-based approach was constructed to encourage multiparty participation of edge services to enhance the efficiency of data processing. Then, an aggregation strategy was proposed to verify and aggregate model parameters to assert the accuracy of decision tree models. Lastly, a data security model based on SM2 public key cryptosystem to accomplish data security and prevent data privacy leakage.

Arafatur *et al.* [A7] introduced a security solution for tackling the problem of designing a secure education Industry 4.0 architecture using microservices. A novel security technique of data transactions was suggested for education microservices using blockchain. The technique includes three phases: blockchain, data sending-receiving, and confidentiality-integrity-availability features, for securing data transmissions of IIoT applications, achieving high performances compared with peer techniques.

IV. Privacy Preservation

Privacy preservation has been widely studied for developing techniques that can secure data sharing and conceal sensitive information from disclosure by unauthorized users. The development of privacy-preserving microservices enables the flexibility and enhances data privacy in IIoT systems [A8]. Jin *et al.* [A9] presented a differential privacy mechanism to secure preserve data sources of 5G and IoT systems. More importantly, the authors suggested a multiple-strategies differential privacy framework based on sparse tensor factorization (STF) (MDP-STF) for securing network traffics of IoT systems network traffic data analysis. MDPSTF includes three differential privacy (DP) mechanisms: DP, concentrated DP, and local DP to strengthen the data privacy of IoT networks.

False data injection attacks (FDIAs) have become a key cyber threat to smart grids. The majority of existing detection techniques have concentrated on learning the temporal relationship of time-series measurement data, without considering the spatial relationship between bus/line measurement data, as well as the relationship between subgrids to efficiently discover FDIA events. Xuefei *et al.* [A10] designed a subgrid-oriented microservice framework via integrating a spatial-temporal neural network for FDIA detection in power systems. First, neural network was developed to train the spatial-temporal relationship of bus/line measurements for subgrids. After that, a microservice-based supervising network is suggested for accumulating the representation features gathered from subgrids for achieving high performance in identifying FDIAs.

V. Edge Computing

There have been attempts to address some challenges of cloud computing via moving the computing resources near to the network edge, named edge computing [A11]. Atonu *et al.* [A12] suggested a secured edge gateway microservices architecture, the so-called SEGA for IIoT-based monitoring systems. The proposed SEGA gateway enables the secure data collection, and transmission and log of data at the network edge. A KNN-based analytical technique was implemented at the edge gateway to learn and infer data at the edge. The technique can effectively infer machine states and monitored parameters of systems, for example, power factor and power consumption.

Mojtaba *et al.* [A13] proposed a two-layer intrusion detection technique to identify attack types from wireless-based metering systems at the edge. The sequential probability ratio testing method was used as a detection engine that discovers attack activities. The detection engine was developed using a random walk that depends on a threshold function that defines the boundaries of attack events at the edge.

Acknowledgment

The Guest Editors would like to thank the authors of all 39 manuscripts for their submissions, as well as subject matter experts who assisted in the reviews and critiques of the submissions. Without their contributions, this Special Section would not have been possible. They would also like to acknowledge the support of the Editor-in-Chief, Prof. R. Luo, and the journal staff for their support and guidance throughout the process.

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

Appendix
Related Articles

[A1] G. Liu, B. Huang, Z. Liang, M. Qin, H. Zhou, and Z. Li, "Microservices: Architecture, container, and challenges," in *Proc. IEEE 20th Int. Conf. Softw. Quality, Rel. Secur. Companion*, 2020, pp. 629–635.

[A2] Q. Qu, R. Xu, S. Y. Nikouei, and Y. Chen, "An experimental study on microservices based edge computing platforms," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2020, pp. 836–841.

[A3] S. Benedict, "Serverless blockchain-enabled architecture for IoT societal applications," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 5, pp. 1146–1158, Oct. 2020.

[A4] N. Moustafa, B. Turnbull, and K.-K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, Jun. 2019.

[A5] M. Abdel-Basset, H. Hawash, and K. Sallam, "Federated threat-hunting approach for microservice-based industrial cyber-physical system," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3091150.

[A6] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in IIoT," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3097131.

[A7] M. A. Rahman, M. S. Abuludin, L. X. Yuan, M. S. Islam, and A. T. Asyhari, "EduChain: CIA-compliant block-chain for intelligent cyber defense of microservices in education Industry 4.0," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3093475.

[A8] N. Bugshan, I. Khalil, N. Moustafa, and M. S. Rahman, "Privacy-preserving microservices in Industrial Internet of Things driven smart applications," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2021.3098980.

[A9] J. Wang, H. Han, H. Li, S. He, P. K. Sharma, and L. Chen, "Multiple strategies differential privacy on sparse tensor factorization for network traffic analysis in 5G," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3082576.

[A10] X. Yin, Y. Zhu, and J. Hu, "A sub-grid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3102332.

[A11] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IOT datasets," *Sustain. Cities Soc.*, vol. 72, 2021, Art. no. 102994.

[A12] A. Ghosh, A. Mukherjee, and S. Misra, "SEGA: Secured edge gateway microservices architecture for IIoT-based machine monitoring," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3102158.

[A13] M. Mohammadi, A. Kavousi-Fard, M. Dabbaghjamanesh, A. Farughian, and A. Khosravi, "Effective management of energy internet in renewable hybrid microgrids: A secured data driven resilient architecture," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3081683.

Nour Moustafa (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from the Faculty of Computer and Information, Helwan University, Helwan, Egypt, in 2009 and 2014, respectively, and the Ph.D. degree in cyber security from the University of New South Wales (UNSW) Canberra, Canberra, ACT, Australia, in 2017.

From February 2019 to July 2021, he was a Lecturer with UNSW Canberra, where he is currently a Senior Lecturer and Postgraduate Coordinator (Cyber) with the School of Engineering and Information Technology (SEIT)UNSW. His research interests include cyber security, in particular, network security, IoT security, intrusion detection systems, statistics, deep learning, and machine learning techniques.

Dr. Moustafa has several research grants with totaling over AUD 1.6 Million. He was the recipient of the 2020 prestigious Australian Spitfire Memorial Defence Fellowship award. He is also an ACM Distinguished Speaker, and CSCRC and Spitfire Fellow. He has served his academic community, as the Guest Associate Editor of IEEE transactions journals, including the IEEE Transactions on Industrial Informatics, IEEE IoT Journal, IEEE Access, *Ad Hoc Networks*, and *Journal of Parallel & Distributed Computing*. He has also served over seven conferences in leadership roles, involving Vice-Chair, Session Chair, Technical Program Committee (TPC) Member, and Proceedings Chair, including 2020–2021 IEEE TrustCom and 2020 33rd Australasian Joint Conference on Artificial Intelligence.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. degree in information security from the Queensland University of Technology, Brisbane, QLD, Australia, in 2006.

He currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio (UTSA), San Antonio, TX, USA.

Dr. Choo is the Founding Co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research & Practice, and the Founding Chair of IEEE Technology and Engineering Management Society's Technical Committee on Blockchain and Distributed Ledger Technologies. He is an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021–2023), and included in Web of Science's Highly Cited Researcher in the field of Cross-Field2020. In 2015, he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He was the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), and the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty.

Adnan M. Abu-Mahfouz (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2005 and 2011, respectively.

He is currently the Centre Manager of the Emerging Digital Technologies for 4IR (EDT4IR) Research Centre at the Council for Scientific and Industrial Research (CSIR), an Extraordinary Professor with the University of Pretoria, the Professor Extraordinaire with the Tshwane University of Technology, Pretoria, and a Visiting Professor with the University of Johannesburg, Johannesburg, South Africa. He participated in the formulation of many large and multidisciplinary R&D successful proposals (as Principal Investigator or main author/contributor). He is the Founder of the Smart Networks collaboration initiative that aims to develop efficient and secure networks for the future smart systems, such as smart cities, smart grid, and smart water grid. His research interests include wireless sensor and actuator network, low-power wide-area networks, software-defined wireless sensor network, cognitive radio, network security, network management, and sensor/actuator node development.

Dr. Abu-Mahfouz is an Associate Editor for IEEE ACCESS, IEEE INTERNET OF THINGS, and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and a Member of many IEEE Technical Communities.