Guest Editorial: AI and Machine Learning Solution Cyber Intelligence Technologies: New Methodologies and Applications

With the recent development of machine learning (ML), artificial intelligence (AI) and cyber technologies in the field of industrial informatics, it is important to migrate the traditional businesses and services in the physical world to the digital cyber-enabled world [item 1) of the Appendix]. Cyber intelligence technologies, such as the fifth-generation (5G) mobile communication network, big data, Internet of Things (IoT), cloud computing, cognitive computing, ubiquitous computing and blockchains, enable goods, houses, services, information, and capitalization to be shared through the Internet [item 2) of the Appendix]. Industrial applications, including various mechanical systems, utilities, supply chains, energy systems, power grids, infrastructures, manufactures, traffics, healthcare, and environmental issues, are partially operated or managed remotely with the influence of AI and cyber intelligence technology [item 3) of the Appendix]. The migration of the traditional business and manufacturing has the following advantages. (1) Predictive control, maintenance, and management can be carried out with analyses of historical sensor data. (2) The levels of security and authentication are enhanced with less human interference. (3) There are human resource, energy, and cost savings because of the activity movement from physical lifestyle to cyber-enabled world lifestyle. (4) The efficiency of the traditional business is improved by automating subprocesses. (5) Both the production volume and quality can be improved using more precise control of the manufacturing process. Under the world-wide pandemic situation caused by the COVID-19 in early 2020, there is an increased demand for people to work or study remotely from home and move all social activities to the online communication systems using the cyber-intelligence technologies. The research areas of cyber-intelligence technologies therefore are incrementally expended, including autonomous vehicles, robotics, cyber manufacturing, communication systems, smart city design, smart facility management, cyber–physical systems (CPS), IoT, smart city, Internet economy, cyber social networks, cyber security, cyber learning, cyber economics, human-machine interaction, blockchain technology, and many others.

The fast development and deployment of AI and cyber intelligence in various industrial areas bring emerging challenges on various aspects. For example, the new AI technology of automated clinical diagnosis creates additional barriers and fears for patients as well as the clinicians. Similar barriers exist in economics, social networks, organizations, and politics. Moreover, the cyber-intelligence technology itself has various technological issues. The problem of handling big data analysis has been discussed for years. It is always challenging to handle big data with limited computational power. The big data storage, security, transportation, and reproductivity are well-known research topics for cloud computing, data communication, networks, and security. A more difficult challenge of AI technologies is the capability of mimicking human thoughts and behaviors using AI systems. Although seriously sophisticated machine learning models, such as the deep learning neural networks, are proposed to investigate human intelligence and simulate human behaviors. It is a mutual agreement that the actual performance of AI is still not reaching the essence of human intelligence. This challenge is also knowns as "adversarial attacks," when disordered inputs are purposely used to test an AI-enabled system, the AI algorithms may respond irregularly or randomly according to human's cognition. While a significant amount of work and research has been undertaken to address various issues in the current development stage of AI and cyber intelligence, all abovementioned challenges and issues continue to change in response to new cyber-intelligence technology developments and clients' demand trends.

This special section of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS intended to survey the recent research developments on consolidating AI, machine learning, and cyber technology for industrial informatics with a focus on cyber intelligence technologies and their applications. Special emphases have been given to novel algorithms, state-of-art methods, hybrid modeling of AI and cyber intelligence related techniques. Selected articles from article submissions of the 4th IEEE Cyber Science and Technology Congress (CyberSciTech 2019, held in Fukuoka, Japan on August 5–8, 2019, http://cyber-science.org/2019/) were invited to submit an extended version to this special section. It is also noted that a notable number of articles from a broad area of science and engineering were received for possible publication consideration. Following a tight review process, we selected nine high-quality article out of over 50 submissions to

Digital Object Identifier 10.1109/TII.2020.2988944

be accepted in this special section. A brief review of all accepted papers is provided as follows.

The first article, "Efficiency evaluations based on artificial intelligence for 5G massive mimo communication systems on high-altitude platform stations," which is contributed by Guan *et al.* [item 4) of the Appendix], focuses on performance improvement of the existing fifth-generation (5G) communication networks on high-altitude platform stations (HAPS). As one of the most important next-generation cyber-intelligence technology, 5G technology has gained enormous attention in recent years. On one hand, the fast development of 5G technology facilitates peoples' lives and makes the cyber-enabled world more engaging. One the other hand, the optimization of 5G technology becomes a new research hot spot in the literature. The 5G technology has not been widely adopted for many countries because of its unstable data transmission and unsatisfied online communication performances. In particular, in a massive multiple input multiple output 5G communication system, package frequencies were different for users under different channel environment, which hinders the 5G technology to be applied to a wide range of different circumstances. In this article , Guan *et al.* leveraged AI-based algorithms, such as the game theory, genetic algorithm (GA) and the particle swarm optimization (PSO) algorithm, to allocate the wireless resources and further solve the above-mentioned problem. In the experiment part, the results showed that the proposed AI technology tuned MIMO communication system has more balanced performance compared with traditional optimization schemes.

The second accepted article is presented by Zhang *et al.* [item 5) of the Appendix] , "Secure transmission of compressed sampling data using edge clouds." The possible integration of data encryption, network security, AI, IoT, and cloud computing is discussed to enhance the data security of cyber-enabled world. A novel data transmission framework is presented for the security of data transmitted from IoT devices to edge cloud to central cloud. Remarkably, the compressed sampling data are split into the sensitive data and the insensitive data in edge cloud. The insensitive data are proved to be perfectly secret. The proposed framework is enabled by a double-layer encryption scheme and a double-layer authentication scheme. A compressive sensing (CS) based encryption algorithm is used to provide the computational secrecy guarantee for the compressed sampling data transmitted from IoT devices to edge servers, and a chaos-based encryption algorithm is proposed to provide the high secrecy guarantee for the sensitive data transmitted from edge servers to central servers. A CS based hash algorithm is designed to guarantee the integrity of the original data, and a chaos-based hash algorithm with tamper localization capacity is designed to guarantee the integrity of the sensitive data as well as the robustness of the signal reconstruction process. The performance of the proposed algorithms is verified with both theoretical analysis and experimental simulation. According to the experimental results, the proposed double-layer encryption scheme provides better secrecy properties than the existing methods. The double-layer authentication scheme can prevent tampering attacks for both the sensitive data and the original signal.

The third article, "Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction" is contributed by Jiang *et al.* [item 6) of the Appendix]. The intelligent control of unmanned aerial vehicles is one of the emerging topics in the field of cyber intelligence. The applications of intelligent UAV control include military functions, plant protection, geological mapping, aerial photographic applications, etc. However, the relatively low cost of illegal deployment of UAVs targeting at military usage becomes one of the main issues in UAV research. The fast advancing of AI and cyber-intelligence technology provides one possible solution of automated authentication of UAV behaviors with secure supervision. The AI and cyber intelligence technologies are adopted to model UAV behaviors based on historical flight data with machine learning and data mining techniques. In the current article, Jiang *et al.* employed the UAV behavior modeling for UAV identity authentication and security supervision. AI techniques, including Kalman filters and Gaussian-processes mechanisms are adopted for behavior prediction and authentication. The proposed framework demonstrates its effectiveness from both theoretical and experimental perspectives. The proposed algorithm has been implemented using a real-world UAV monitoring system. A comprehensive comparative study has been conducted to compare the proposed framework with time series classification methods based on Shapelet tree, benchmark data classification methods, classification methods based on probabilistic reasoning, integrated learning classification methods and Shapelet learning classification methods to show the superior prediction accuracy and improved efficiency.

The fourth paper, "Privacy-enhanced data collection based on deep learning for internet of vehicles" is contributed by Wang *et al.* [item 7) of the Appendix]. The possibility of combining deep learning and edge computing in Internet of Vehicles (IoV) is discussed to reduce communication bandwidth and latency to protect user privacy. A data collection strategy based on edge computing is proposed to solve the high delay problem of vehicle data uploading to cloud in IoV. In the new data collection framework, by analyzing the historical data of network quality of service (QoS), a new vehicle-mounted network QoS evaluation model is constructed. The terminal data is uploaded adaptively according to the evaluation results. Based on a semi-supervised learning approach and the idea of image fingerprint, the correlation and similarity of image information in the IoV are detected. In the process of data collection, irrelevant data and data with large similarity are eliminated in real time, effectively reducing the amount of data uploaded to the cloud server. At the meanwhile, because of the federal learning technology, the cloud collects the training results on each edge device instead of the original data from end users directly, which maximizes the protection of user privacy. According to the experimental results, the proposed scheme significantly reduces the amount of data uploaded to the cloud and effectively protects users' data privacy.

The fifth accepted article, "Learning URL embedding for malicious website detection" is contributed by Yan *et al.* [item 8) of the Appendix]. The article discusses the security of

cyberspace caused by the surge of intelligent network equipment. A novel feature extraction framework is proposed for dealing with massive malicious domain names. It is worthwhile noted that the machine learning technique helps identify malicious domain names hidden in huge data more easily. The extraction of high-quality features greatly improves the performance of the original machine learning model. Due to the fact that feature engineering tasks may have the interferences to subjective factors, resulting in "curse of dimensionality," an unsupervised learning mechanism based on URL embedding is designed to overcome the abovementioned problem. Significant improvements have been achieved on feature extraction results of malicious domain names, which further improve the performance of malicious domain name detection. A deep neural network model combining time series analysis is designed to establish and store the mapping between URL and its corresponding distributed representation, to further improve the feature extraction results of malicious domain names. This paper explores the key parameters of the URL embedding model, solves the interference of human subjective factors and "curse of dimensionality" caused by feature engineering, and effectively improves the performance of malicious domain name recognition. The performance of the proposed algorithms is justified using both theoretical analysis and experimental simulation.

The sixth article with the title "Fault location technology for power system based on information about the power Internet of Things," presented by Kong *et al.* [item 9) of the Appendix], employs the AI and cyber-intelligence technology to locate and diagnose faults for power distribution systems, which is one of the long existing topics in the field of power IoT. The complexity of the power distribution system hinders the application of modern IoT technology. Various data sets are collected using different resources, resulting in data wastage and impactable problems. An efficient and effective fault monitoring, warning and management system is highly demanded under this context. In this article, Kong *et al.* performed data analysis on distribution phasor measurement unit (D-PMU) information, sensor data and network symmetry characteristics to develop an intelligent control system on power IoT. The T-connection problem is considered and resolved. Fault types are identified together with the zone and branch information. A series of experiments are carried out to test the influence factors of fault distance, fault resistance, D-PMU information on fault location identification. Two conclusions are drawn from the authors. First, the accuracy of the fault location and diagnosis depends on the accuracy of D-PMU information. The interconnection information in the power IoT system raises incremental difficulties to identify fault locations and types. The proposed method can be further extended to other fault location and diagnosis areas.

The seventh article, "Edge computing based channel allocation for deadline-driven IoT networks" is presented by Gao *et al.* [item 10) of the Appendix]. Edge-based channel allocation for IoT networks is discussed for improving the reliability of packet transmissions with pre-assumed deadline constraints. In the proposed framework, a novel prioritization metric is first presented to allocate time slots and channels, in which deadline urgency and wireless collisions are considered. After that, an adaptive scheme is proposed to make use of the spare slots for possible retransmissions on the unreliable links, which further improves the overall transmission reliability. In the above framework, link quality prediction and allocation decisions are two key modules. However, the resource-constrained IoT nodes cannot afford the energy consumption of accurate but complex learning-based implementations of those modules. Therefore, this article proposes to employ the edge computing framework and offload the link prediction and decision-making to the edge servers. Then an RNN-based algorithm is developed and employed on edge servers to predict the link quality for allocation decisions, which achieves high accuracy compared to the existing heuristics on link estimation. In this way, the energy consumption is mitigated from IoT devices to the edge servers, and accurate channel allocation and adaptive retransmission schedules can be achieved simultaneously. The performance of the proposed algorithms is verified with both simulation and testbed experiments. According to the evaluation results, the proposed channel allocation scheme achieves better performance in terms of packet delivery ratio before deadline (PDR-BD) compared to the existing methods.

To achieve both the effective and efficient performance of Deep Recurrent Neural Network (DRNN) based human activity recognition (HAR), especially deployed on the resource-constrain smartphones, the eighth accepted article "PSDRN: An efficient and effective HAR scheme based on feature extraction and deep learning," which is presented by Li *et al.* [item 11) of the Appendix], proposed the power spectral density based recurrent neural network (PSDRNN) and tri-axle accelerated PSDRNN (TriPSDRNN) schemes. In the PSDRNN scheme, the power spectral density (PSD) features are efficiently extracted from smartphone's linear accelerations. Furthermore, in the TriPSDRNN scheme, tri-axle accelerations are explicitly employed before DRNN classification model. As a result, the extracted PSD features can be effectively utilized to capture the frequency characteristics and meanwhile retain the successive time characteristics of smartphone accelerometer data, which consequently improves the LSTM-based HAR classification significantly. The thorough experiments on a real data set demonstrate that PSDRNN can achieve the comparable effectiveness as the *xyz*-DRNN (the most accurate DRNN based HAR scheme only using acceleration data), and the average recognition and training time is significantly reduced. Moreover, the TriPSDRNN scheme demonstrates superior performance over the *xyz*-DRNN in terms of recognition accuracy, and the running time (computational complexity) is still lower than *xyz*-DRNN. In addition, the proposed PSDRNN scheme achieved superiority in the recognition of complex transition activities, based on the fact of extracting PSD from the linear scalar acceleration data.

The last article is presented by Zhu *et al.* [item 12) of the Appendix] with the title "AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection," where the cyber intelligence application on image security is discussed.

In many real-world applications, the authenticity and integrity of digital images should be protected to avoid misleading changes, fraud, and copyright disputes. Copy-move is a commonly tampered operation in image forgery. In this study, an end-to-end neural network is proposed based on Adaptive attention and Residual refinement Network (AR-Net), which includes a detection module to get coarse tampered mask and a residual refinement module to optimize the boundary of predicted mask. To fully capture context information and enrich the representation of features, the position and channel attention features are fused by the adaptive attention mechanism. In addition, the predicted coarse mask is optimized through the residual refinement module, which retains the structure of objects boundary. The extensive experiments are evaluated on CASIAII, COVERAGE, and CoMoFoD data sets and show that the performance of the proposed algorithm is superior to the state-of-the-art algorithms. The proposed algorithm can effectively locate tampered regions, and impose high robust performance on post-processing operations.

To conclude, the guest editors would like to thank all authors submitting their valuable works to this special section of IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII), which contributed significantly to the literature of AI and cyber intelligence applications in the field of industrial informatics. We are also grateful to the editorial board members as well as all the reviewers for their great effort reviewing the submitted articles, providing constructive recommendations and assisting the editors to make the final decision. We also would like to send our special thanks to the editor-in-chief (EIC), Prof. Ren Luo and the administrative staff of the journal, Lisa and Linda, for their precious time and instructions that help us prepare and finalize this special section.

KE YAN, *Guest Editor*
College of Information Engineering
China Jiliang University
Hangzhou 310018, China

LU LIU, *Guest Editor*
School of Informatics
University of Leicester
Leicester LE17RH, U.K.

YONG XIANG, *Guest Editor*
School of Information Technology
Deakin University
Burwood, VIC 3125, Australia

QUN JIN, *Guest Editor*
Department of Human Informatics and Cognitive Sciences
Waseda University
Tokorozawa 359-1192, Japan

APPENDIX
RELATED WORK

1) A. Ebrahimzadeh and M. Maier, "Tactile internet over fiber-wireless–enhanced LTE-A hetnets via artificial intelligence-embedded multi-access edge computing," *5G-Enabled Internet Things*, Ch. 17, pp. 355–374, 2019.
2) K. Yan, W. Shen, Q. Jin, and H. Lu, "Emerging privacy issues and solutions in cyber-enabled sharing services: From multiple perspectives," *IEEE Access*, vol. 7, pp. 26031–26059, 2019.
3) G. Aceto, V. Persico, and A. Pescapé, "A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges," *IEEE Commun. Surv. Tut.*, vol. 21, no. 4, pp. 3467–3501, Oct./Dec. 2019.
4) M. Guan *et al.*, "Efficiency evaluations based on artificial intelligence for 5G massive MIMO communication systems on high-altitude platform stations," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6632–6640, Oct. 2020.
5) Y. Zhang, P. Wang, L. Fang, X. He, H. Han, and B. Chen, "Secure transmission of compressed sampling data using edge clouds," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6641–6651, Oct. 2020.
6) C. Jiang, Y. Fang, P. Zhao, and J. Panneerselvam, "Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6652–6662, Oct. 2020.
7) T. Wang *et al.*, "Privacy-enhanced data collection based on deep learning for Internet of vehicles," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6663–6672, Oct. 2020.
8) X. Yan, Y. Xu, B. Cui, S. Zhang, T. Guo, and C. Li, "Learning URL embedding for malicious website detection," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6673–6681, Oct. 2020.
9) X. Kong, Y. Xu, Z. Jiao, D. Dong, X. Yuan, and S. Li, "Fault location technology for power system based on information about the power Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6682–6692, Oct. 2020.
10) W. Gao, Z. Zhao, Z. Yu, G. Min, M. Yang, and W. Huang, "Edge-computing-based channel allocation for deadline-driven IoT networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6693–6702, Oct. 2020.
11) X. Li, Y. Wang, B. Zhang, and J. Ma, "PSDRNN: An efficient and effective HAR scheme based on feature extraction and deep learning," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6703–6713, Oct. 2020.
12) Y. Zhu, C. Chen, G. Yan, Y. Guo, and Y. Dong, "AR-Net: Adaptive attention and residual refinement network for copy-move forgery detection," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6714–6723, Oct. 2020.

Ke Yan (Member, IEEE) received the bachelor and Ph.D. degrees in computer science from the School of Computing (SoC), National University of Singapore (NUS), Singapore in 2006 and 2012 respectively.

He worked with the Masdar Institute of Science and Technology (MIST) campus, Khalifa University, Abu Dhabi, UAE as a Postdoctoral Researcher from 2012 to 2014. He was an Associate Professor in China Jiliang University, Hangzhou, China and is currently an Assistant Professor of School of Design and Environment (SDE), NUS. He has been the leading/corresponding guest editor of a special issue named "Machine Learning for AI-Enhanced Healthcare and Medical Services: New Development and Promising Solution" with the journal IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB) from June 2018 to May 2020. He is actively engaged in cross-discipline research fields, including machine learning, artificial intelligence, cyber intelligence, applied mathematics, sustainability, applied energy and etc. He has published more than 40 full length papers with highly ranked conferences and journals, such as International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS), Association for the Advancement of Artificial Intelligence (AAAI), IEEE Transactions on Sustainable Energy (TSE), IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS: SYSTEMS (SMCA), IEEE ACCESS, *Applied Energy* (AE), *Future Generation Computer Systems* (FGCS), *Energy and Buildings* (ENB), *Building and Environment* (BAE), and *International Journal of Refrigeration* (JIJR).

Lu Liu received his Ph.D. degree in computer science from Surrey Space Centre at the University of Surrey, Guildford, UK, in 2008.

He is currently the Head of the School of Informatics at the University of Leicester, Leicester, UK. He had worked as a Research Fellow at the WRG e-Science Centre at the University of Leeds, Leeds, UK. He has secured many research projects which are supported by research councils, BIS, Innovate UK, British Council and leading industries. His current research interests are in the areas of data analytics, service computing, cloud computing, Artificial Intelligence and the Internet of Things and has over 200 scientific publications in reputable journals, academic books and international conferences.

Dr. Liu received the Vice-Chancellor's Awards for Excellence in Doctoral Supervision in 2018, BCL Faculty Research Award in 2012 and was recognized as a Promising Researcher by the University of Derby in 2011. He has been the recipient of 6 Best Paper Awards from international conferences and was invited to deliver 7 keynote speeches at international conferences. He is a Fellow of British Computer Society (BCS) and currently serves as an Editorial Board Member of 6 international journals and the Guest Editor for 12 international journals. He has chaired over 30 international conference and workshops, and presently or formerly serves as the program committee member for over 60 international conferences and workshops.

Yong Xiang (Senior Member, IEEE) received his B.E. degree in electronic engineering and M.E. degree in communications and electronic system from the University of Electronic Science and Technology of China, Chengdu, China in 1983 and 1989 respectively, and Ph.D. degree in electrical and electronic engineering from The University of Melbourne, Melbourne, Australia in 2003.

He is a Professor at the School of Information Technology, Deakin University, Melbourne. He is also the Director of Deakin University.-Southwest University Joint Research Centre on Big Data, the Director of Data to Intelligence Research Centre, and the Director of Deakin Blockchain Innovation Lab. He has published 5 monographs, over 150 refereed journal articles (mainly in IEEE journals), and over 85 conference papers in these areas. He is the co-inventor of 2 U.S. patents and some of his research results have been commercialised. His research has been strongly supported by various funding bodies through many awarded research grants, including 6 ARC Discovery and Linkage grants from the Australian Research Council. His current research interests include information security and privacy, signal and image processing, data analytics and machine intelligence, Internet of Things, and blockchain

Prof. Xiang is a Senior Area Editor of IEEE SIGNAL PROCESSING LETTERS and Associate Editor of IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and IEEE ACCESS. He served as Guest Editor for a number of journals, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE MULTIMEDIA MAGAZINE, etc. He has been invited to give keynote speeches and served as General Chair, Honorary Chair, Program Chair, TPC Chair, Symposium Chair, Track Chair, and Session Chair in many international conferences.

Qun Jin (Senior Member, IEEE) received the B.S. degree from Zhejiang University, China in 1982, and the Ph.D. degree from Nihon University, Japan in 1992. He is currently a Professor at the Networked Information Systems Laboratory, Department of Human Informatics and Cognitive Sciences, Faculty of Human Sciences, Waseda University, Japan. He is currently the Dean of Graduate School of Human Sciences, and the Deputy Dean for International Affairs, Faculty of Human Sciences. He has been extensively engaged in research works in the fields of computer science, information systems, and human informatics. He authored or co-authored several monographs and more than 300 refereed papers published in the world-renowned academic journals, such as IEEE INTERNET OF THINGS JOURNAL, ACM Transactions on Intelligent Systems and Technology, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, IEEE/ACM TRANSACTIONS ON COMPUTATIONAL BIOLOGY AND BIOINFORMATICS, and IEEE SYSTEMS JOURNAL, and international conference proceedings, among which a few were granted best paper awards. His current research interests cover human-centric ubiquitous computing, behavior and cognitive informatics, big data, personal analytics and individual modeling, intelligence computing, blockchain, cyber security, cyber-enabled applications in healthcare, and computing for well-being.

Prof. Jin served as a Guest Editor for numerous academic journals and magazines, such as IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, IEEE MULTIMEDIA, IEEE CLOUD COMPUTING, and *Information Sciences (Elsevier)*, and served as a general chair and program chair for many international conferences. He is a Foreign Member of the Engineering Academy of Japan (EAJ).