Editorial

Syed Hassan Ahmed*

Computer Science Department,
California State University,
Fullerton, CA 92831, USA
Email: sh.ahmed@ieee.org
*Corresponding author

Murad Khan

Department of Computer Science and Engineering,
Kuwait College of Science and Technology,
Kuwait City, Kuwait
Email: m.khan@kcst.edu.kw

Wael Guibene

Amazon Web Services (AWS),
Dallas-Fort Worth Metroplex, Texas, USA
Email: wael.guibene@ieee.org

Biographical notes: Syed Hassan Ahmed is IEEE and ACM Senior Member as well as ACM Distinguished Speaker since 2018. Currently, he is managing mobile, compute, and connectivity products at Qualcomm Inc. In addition, he is also an adjunct faculty member at California State University, Fullerton Campus, where he teaches computer science courses to graduate classes. Previously, he was with JMA Wireless as a Product Specialist for Distributed Antenna Systems (DAS), CBRS, Private LTE, Digital Electricity, and open RAN product lines. Prior to this assignment, he was an Assistant Professor in the Department of Computer Science at Georgia Southern University, USA, where, he also founded the Wireless Internet and Networking Systems (WINS) lab.

Murad Khan is an Assistant professor in the Department of CSE at the Kuwait College of Science and Technology, Kuwait. He received his MS and PhD degrees from Kyungpook National University, South Korea, in 2017. Before joining the KCST, he worked as a Korea Research Fellow with the School of Computer Science & Engineering, Kyungpook National University, South Korea. His research expertise includes designing energy-efficient communication protocols for the Internet of Things using machine and deep learning techniques. He has published more than 100 research articles in top-tier journals and international conferences.

Wael Guibene is a Sr. Partner Solutions Architect at AWS focusing on IoT & Hybrid Edge Services. Prior to his position at AWS, he was Principal System Architect - IoT, Compute and Wireless Solutions at Infineon driving design wins for Matter-enabled 1st generation products (connected lights, locks and sensors). Prior to that, he was Lead IoT Standardisation at Samsung Electronics working on CSA's Matter standard (Technical and Marketing groups Rep). Prior to joining SEA, he worked for Charter Communications where he was a Principal Engineer in charge of the standardisation and PoCs for IoT (LoRaWAN and private-LTE/CBRS).

Blockchain technologies have been continuously attaining attention from people from different scenarios. For instance, blockchain is being used in sectors like banking, investing, crypto-mining etc. Blockchain is essentially an atypical database that stores data as blocks. These blocks of data are chained to each other in a chronological fashion, hence the name blockchain. Now, blockchain is seen as a promising solution towards solving the trust and privacy issues that might arise with the introduction of sixth-generation (6G) wireless communication networks. Blockchain can seamlessly offer various benefits, including trust among network entities, secure access control and management, efficient and encrypted resource sharing, privacy protection etc., due to its inherent capabilities such as decentralisation, anonymity, immutability, and resiliency.

Blockchain can serve as a solution for various cases and applications. Among them, in 5G and 6G, wireless communication networks are resource sharing via the networks. Practically, it is often not feasible to expect or receive the same amount of cooperation or coordination from the receiver or the host in terms of privacy, cost, security etc. But blockchain technologies can effectively handle all the complexities that are associated with resource sharing due to the advent or presence of software-defined networks, cloud computing, network function visualisation (NVF) etc. Also, blockchain can be a potential solution to problems in spectrum sharing. Some verification protocols can ensure secure spectrum sharing in mobile cognitive radio networks. Further, blockchain systems can autonomously control and monitor unregistered spectrums.

Computing and storage of network data is another field that has a huge potential for blockchain technologies in the future wireless communication networks and technologies. The future 6G wireless communication networks can largely depend on B-RAN which acts as a unified interface for resource pooling and sharing of data in a trusted and secure manner. Apart from these, blockchain can be used as an important tool in network infrastructure, network slicing, data interaction between trusted sources, credibility in identity, the authenticity of shared data, secure and device access control, system access control, data access control, privacy protection, the privacy of identity and data, tracing, certification and supervision, etc. The full potential of blockchain can only be discovered through collective effort and extensive research in areas like blockchain for wireless networks with cognitive abilities and the security and privacy of blockchain databases. This call for papers has resulted in the acceptance of 11 articles, and they are introduced in the following, highlighting their major contributions.

In the article "High-speed pre-accumulator and post-multiplier for convolution neural networks with low power consumption", the authors present an artificial intelligence-based convolutional neural network algorithm for energy-efficient wireless communication. This is made through the implementation of Pre-Accumulator and Post-Multiplier's algorithms. The next article is entitled "Congruent fine-grained data mining model for large-scale medical data mining". This work deals with efficient electronic multimedia generated from cloud computing and Internet of Things (IoT) platforms. A congruent-fine grained data mining model is proposed to attain the intended objectives. The next article is entitled "Priority-based SenCar deployment strategy for mobile sink data gathering in WSN". It aims to resolve the various challenges associated with data gathering across mobile sinks in wireless sensor networks. A priority-based sensor deployment strategy is proposed to attain these objectives.

In the article "Machine learning-based security active defence model – security active defence technology in the communication network", Machine Learning-based Security Active Defence Model (MLSADM) is proposed to incorporate security and privacy measures across the wireless sensor networks. This approach effectively prevents various security threats and helps in more secure communication across wireless sensor networks. The next article is entitled "Processing power sharing using a gadget 'Power Save' for downloading scientific research projects". In this work, an efficient power saving algorithm using cloud computing and smart mobile devices is proposed. The objective here is to provide energy-efficient wireless sensor communication. The next article is entitled "Blockchain-based system for storage utilisation and secure sharing of EHR data". This work provides an optimised approach for secure data storage and access across the EHR applications. This approach is highly resistant to cyber threats and provides improved security measures.

In the article "Internet of vehicle things communication based on big data analytics integrated internet of things", the author converges big data techniques and IoT for efficient data transmission across the Internet of Vehicle networks. This is made through the implementation of big data analytics integrated IoT framework. The next article is entitled "Secure dynamic bits standard scheme in private cloud environment", the author attempts to address the security challenges across the private cloud environment. This is made through the implementation of the standard data encryption algorithms. The performance of this approach is found to be comparatively better than the existing approaches. The next article is entitled "A one-dimensional superior logistic map based-image encryption". This work presents a one-dimensional superior logic map based image encryption algorithm for securing communication across the wireless sensor networks. The scheme was evaluated against numerous standard measures, and it offers comparatively better results.

The next article is entitled "Enhanced-KNN (M-KNN) based outlier detection and sensor data aggregation for large data streams in the IoT-cloud". This approach makes use of the data aggregation and dimensionality reduction techniques to secure the channel of data transmission with improved accuracy. Modified K-nearest neighbour algorithm and principal component analysis algorithms are used for this purpose. In the final article "Efficient authentication method using binary search tree with multi-gateway in wireless IoT", the authors aim to focus on the security measures associated with IoT systems. The authors proposed an efficient authentication method using binary search tree algorithms for securing the process of data transmission across the IoT gateways.

To conclude, the guest editors would like to thank all the authors and reviewers for their valuable contributions. We are confident that the research articles presented in this special issue will add significant value to the scientific community and assist in interesting future research applications.