Guest Editorial: Blockchain and Healthcare Computing

WITH the development of society, health has received increasing attentions. The development of science and technology has also promoted the protection of health. In recent years, the rapid development of computing and networking technologies has improved the ability to collect, measure, and analyze health-related data, and thus tremendous opportunities have opened up for healthcare computing. Meanwhile, these technologies have also brought new challenges and issues. For example, patients' diagnostic records stored in hospital management systems may be tampered with, which may affect the patients' health management and insurance compensation.

Blockchain has received increasing attention from academia and industry in recent years. It enables transparent interactions of different parties in a more secure and trusted network. The traceability of blockchain allows data to be retained on the blockchain from every step of the data generation process, to endorse the quality of the data and to ensure the correctness of data analysis and mining. The content recorded in the blockchain cannot be tampered with, so it can be used to record important information in health management, provide accurate and reliable health knowledge for network users, and provide accurate information for auditing.

After a rigorous review process, 4 articles have been selected for publication in this special issue, which are briefly discussed as follows.

In any healthcare system in today's society we see a strong sense of inter-connectivity maintaining relationships between patients, healthcare practitioners, medical devices, and staff. Using the Internet-of-Things (IoT) infrastructure in these health systems means that connected devices on these systems must be authenticated and securely interconnected to minimize security and privacy breaches from within a given network. In the first article, entitled "Decentralized Authentication of Distributed Patients in Hospital Networks using Blockchain", Yazdinejad *et al.* proposed a novel decentralized authentication of patients in a distributed hospital network, by leveraging blockchain technology. They showed that the proposed architecture's decentralized authentication does not require re-authentication as devices may move around in a distributed network setting. This improvement provided a considerable impact on increasing throughput, reducing overhead, improving response time, and decreasing energy consumption in the network which they showed through in-depth experimental results. The authors also provided a comparative analysis of the model with and without blockchain to show the overall effectiveness of the proposed solution.

To enable users have ownership of their own medical data and share their medical data safely and dynamically between different medical institutions, in the second article, entitled "Dynamic Autonomous Cross Consortium Chain Mechanism in e-Healthcare", Qiao *et al.* proposed a solution for achieving dynamic communication between medical consortium chains. Specifically, in this paper, the authors developed a cross-chain communication mechanism by simplifying the heterogeneous node communication topology and the construction rules of the node identify credibility path-proof to carry out dynamic construction and verification of the path-proof for cross-domain transactions. Experimental results showed that the proposed approach can not only enable patients to share their records safely and autonomously in an authorized medical consortium chain within milliseconds but also realize dynamic adaptive interaction.

In the third article, entitled "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology", Zhuang *et al.* proposed a patient-centric health information exchange (HIE) scheme based on blockchain to address the challenges of security and privacy concerns, data inconsistency, and timely access to the right records across multiple healthcare facilities. They conducted a large-scale simulation of this patient-centric HIE process and quantitatively evaluated the model's feasibility, stability, security, and robustness.

Coronary heart disease (CHD) is currently one of the most common type of heart diseases and there are more than 370,000 deaths every year because of CHD. In the last article, entitled "Blockchain-Enabled Contextual Online Learning under Local Differential Privacy for Coronary Heart Disease Diagnosis in Mobile Edge Computing", Liu *et al.* studied how to assist doctors to make proper clinical diagnosis of CHD based on the mobile edge computing. However, it faces many challenges, including personalized diagnosis, high dimensional datasets, clinical privacy concerns and insufficient computing resources. To solve the above-mentioned problems, this paper proposed a novel blockchain-enabled contextual online learning model under local differential privacy for CHD diagnosis in mobile edge computing. The approach is based on an adaptively expanding tree structure to support increasing datasets of medical diagnosis records (MDR), which also ensures the accurate diagnosis recommendation results. The local differential privacy method is used to prevent the privacy of patients from being attacked and utilize the blockchain-enabled model to guarantee the security of diagnosis records sharing and medical transactions. Based on real experiments, the proposed algorithm outperformed related context-aware privacy-preserving approaches by about 21% in

Digital Object Identifier 10.1109/JBHI.2020.3003767

terms of error rate when the regret is sublinear and 31% in terms of running time, which is a significant advancement in this field.

We foresee the continuation of the use of blockchain in healthcare computing and recognize that this special issue cannot cover all emerging issues in this area. We sincerely thank all the authors and reviewers for their efforts, and the Editor-in-Chief and Staff Members for their gracious support. We hope that the readers will enjoy this special issue.

YULEI WU, *Guest Editor*
College of Engineering, Mathematics and Physical Sciences
University of Exeter, United Kingdom
y.l.wu@exeter.ac.uk

ZHENG YAN, *Guest Editor*
School of Cyber Engineering
Xidian University, China
Department of Communications and Networking
Aalto University, Finland
zheng.yan@aalto.fi

F. RICHARD YU, *Guest Editor*
School of Information Technology
Carleton University, Canada
RichardYu@cunet.carleton.ca

ROBERT DENG, *Guest Editor*
School of Information Systems
Singapore Management University, Singapore
robertdeng@smu.edu.sg

VIJAY VARADHARAJAN, *Guest Editor*
Faculty of Engineering and Built Environment
The University of Newcastle, Australia
vijay.varadharajan@newcastle.edu.au

WEI CHEN, *Guest Editor*
Department of Electronic Engineering
Fudan University, China
w_chen@fudan.edu.cn