IEEE JOURNAL OF

BIOMEDICAL AND HEALTH INFORMATICS

J-BHI Special Issue on "Federated Learning for privacy preservation of Healthcare data in Internet of Medical Things"

Due to the advancements in Internet of Medical Things (IoMT), wearable devices, remote monitoring of patients is possible like never before. Machine learning and deep learning techniques help the doctors immensely in remotely diagnosing the patients by learning the patterns from the data generated through these devices. The main problem with traditional machine learning (ML)/deep learning (DL) models is that the data from the individual devices, sensors, wearables from patients have to be transferred to the central servers to train the data using the ML/DL models. Due to the sensitive nature of the healthcare data, the aforementioned approach of transferring the patients' data to the central servers may create serious security and privacy issues.

Federated learning is a recent variant of ML, where, instead of transferring the data to the central servers, the ML model itself is deployed to the individual devices to train on the data. The parameters from the models trained on individual devices can then be sent to the central ML/DL model for global training. In this way, federated learning can help in preserving the privacy of the patient's data by not exposing the sensitive information to the potential intruders, hackers. At present, the coronavirus pandemic has expanded to a worldwide health emergency and poses a threat to millions of people. To combat coronavirus, related researchers have used the emerging machine learning technologies to train a model for disease prediction or diagnosis. However, due to the unreliable communication channels and potential attackers, a large amount of collected data may incur many security and privacy concerns during this period. Aiming to guarantee patient record security in the transfer and training process, privacy-preserving federated learning becomes a better choice. Therefore, in this issue, we would like to gather some high-quality papers that utilize cutting-edge federated learning technology to secure the healthcare data and give some helpful reference to the current society.

This special issue solicits quality research papers on application of federated learning for securing the healthcare data generated through IoMT. Experimental results, case studies, review/survey papers on federated learning for Internet of Medical Things are welcome.

1. Privacy and security issues in IoMT.
2. Applications of federated and distributed learning in preserving the privacy of the medical data.
3. Architecture of Federated Learning in IoMT.
4. Architectures of blockchain and federated learning in IoMT.
5. Case studies of federated learning in IoMT.
6. 5G and beyond for federated learning in IoMT.
7. Edge and fog computing integrated with federated learning for IoMT applications.
8. Federated learning for intrusion detection in IoMT.
9. Big data analytics for federated learning in IoMT

References:

1. Jin, H., Dai, X., Xiao, J., Li, B., Li, H., & Zhang, Y. (2021). Cross-Cluster Federated Learning and Blockchain for Internet of Medical Things. IEEE Internet of Things Journal.
2. Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance enhanced Internet of health things framework: A blockchain managed federated learning approach. Ieee Access, 8, 205071-205087.
3. Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated Learning-based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal.
4. Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619-640.
5. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Bhattacharya, S., ... & Gadekallu, T. R. (2021). Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions. arXiv preprint arXiv:2106.09527.
6. Pham, Q. V., Dev, K., Maddikunta, P. K. R., Gadekallu, T. R., & Huynh-The, T. (2021). Fusion of federated learning and industrial internet of things: a survey. arXiv preprint arXiv:2101.00798.
7. RM, S. P., Maddikunta, P. K. R., Parimala, M., Koppu, S., Gadekallu, T. R., Chowdhary, C. L., & Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Computer Communications, 160, 139-149.

Guest Editors

1. Thippa Reddy Gadekallu, Vellore Institute of Technology, India, E-mail: thippareddy.g@vit.ac.in
2. Mamoun Alazab, Charles Darwin University, Australia, E-mail: alazab.m@ieee.org
3. Jude Hemanth, Karunya Uiversity, India, E-Mail: judehemanth@karunya.edu (Associate Editor, JBHI)
4. Weizheng Wang, City University of Hong Kong, Hong Kong, E-mail: weizheng.wang@ieee.org

Key Dates

Deadline for Submission: 31 December, 2021
First Reviews Due: 1 March, 2022
Revised Manuscript Due: 1 May, 2022
Final Decision: 1 August, 2022