Guest Editorial
Federated Learning for Privacy Preservation of Healthcare Data in Internet of Medical Things and Patient Monitoring

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 [1]. The main problem with traditional machine learning (ML)/deep learning (DL) models is that the data from the individual devices, sensors, wearables of 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 (FL) 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 [2]. 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, FL 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 [3], [4], [5]. 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 FL becomes a better choice [6], [7].

From the above backdrop, this special issue aims to gather high-quality research works that utilize cutting-edge FL based technologies to secure the healthcare data, as well as preserve the privacy of sensitive data generated from IoMT and give some helpful reference to the current society. The papers accepted in this special issue are summarized below.

The first paper from Xu et al. [A1] proposed an FL based approach to reduce the network scale through quantization of the neural network parameters. The proposed FEDMSQE, FL with Minimum Square Quantization Error, addresses the challenge of deploying extensive neural network models on IoMT devices. FEDMSQE ensures that least quantization error is achieved by individual clients in the FL setting. The results obtained from the proposed FL based methodology ensures the reduction of transmission cost with improved security.

In the next work, Lakhan et al. [A2] proposed a novel approach, FL-BETS to find and ensure that the privacy of the healthcare data and the potential frauds at various levels such as remote nodes and fog nodes are identified in a timely manner. The proposed FL-BETS ensures the minimum energy consumption and delay in healthcare workloads.

IoMT facilitates healthcare services such as saving the healthcare records and monitoring the health of the patients in real-time. The sensors in these IoMT based applications can be used to classify several diseases in the patients. These applications based on IoMT use mobile devices that roam across various locales dynamically. However, these apps face two significant challenges such as cost of application execution services and also the breach of sensitive healthcare data. To address these issues, Lakhan et al. [A3] proposed a mobility-aware security dynamic service composition (MSDSC) algorithmic framework for workflow healthcare which relies on restricted Boltzmann machine and serverless mechanisms. This study suggests the training of probabilistic models at each phase of the stochastic deep neural network in IoMT. The proposed FL based methodology ensures task sequencing, service composition, scheduling, and security in IoMT based applications.

The usage of smartphones has significantly increased as many tasks can be performed through it in our daily lives. The vibrations generated through typing on a smartphone's keyboard can be used in identifying typed keys that may result in side channel attacks. Sensitive data like personal medical information, clinical nodes, username and password may be collected through the hardware sensors available in the smartphones. The study by Rehman et al. [A4] proposed an FL based framework for detecting side-channel attacks in smartphones to secure the sensitive medical information.

Ahmed et al. [A5] presented an overview of different FL based architectures that can be used for FL-enabled IoMT. They also discussed about how the physical layer security to preserve privacy of data in FL enabled IoMT with relevant case study. They presented recent state of the art in this area and highlight several challenges and open issues related to physical layer security assisted FL enabled IoMT.

Date of current version 6 February 2023.
Digital Object Identifier 10.1109/JBHI.2023.3234604

Two of the major issues concerning the penetration of IoMT are privacy preservation of sensitive healthcare information and the isolation of medical systems as the scope of activities from users is bounded within the system and it is relatively difficult to share the data of on medical system with others. Xu et al. [A6] proposed a blockchain based attribute-based encryption (ABE) mechanism to solve these two issues. ABE breaks the boundaries of the system that enables the sharing of data among the medical institutions and also preserve privacy of the sensitive information in healthcare systems.

IoMT plays a major role in improving user experience in critical applications such as remote diagnosis in near real-time. However, security and privacy problems are major challenges in IoMT. Most of the existing solutions for misbehavior analysis suffer from privacy concerns. Rahmadika et al. [A7] proposed a blockchain and FL based framework to preserve the privacy for secured detection of misbehavior in IoMT devices, especially in artificial pancreas system. The proposed method uses a privacy-preserving bidirectional LSTM supplemented with blockchain technology that ensures security.

In another interesting work, Singh et al. [A8] proposed a Dew-Cloud based framework for enabling hierarchical FL. This framework provides a greater level of privacy preservation along with higher availability of critical applications based on IoMT. In this framework, a hierarchical LSTM at distributed Dew servers are supported by cloud computing in the backend.

In the next work, Wang et al. [A9] proposed a novel efficient encrypted parallel ranking search system that ensures efficient retrieval without leaking the privacy in cloud computing when dealing with massive amounts of medical data generated through IoMT. The authors designed a parallel binary search tree structure for the block and a parallel retrieval algorithm is proposed that is adaptable for the proposed structure. The feature vectors that are generated through the proposed scheme are highly difficult to be reversely analyzed due to their unexplainability that enhances the privacy preservation of the data from researchers and the patients.

Rachakonda et al. [A10] provided a unique architecture for FL, which enables collaborative learning across dispersed sites without transferring data. Scalability, data security, aggregation, and production readiness are addressed. The proposed approach uses multi-party computation to avoid reverse engineering attacks across devices and silos. In one use case, the system is employed in an AI-driven IoMT environment and benchmarked against conventional centralized training. The framework may be easily applied in clinical use scenarios.

In FL, a distributed machine learning methodology where numerous devices or computers work together to train a model without sharing their data, Li et al. [A11] proposed a technique for recreating input data. End-to-End Gradient Inversion (E2EGI), the suggested approach, is based on a novel optimization method known as Minimum Loss Combinatorial Optimization (MLCO). E2EGI can execute gradient inversion attacks (GIA) on deep network models and ImageNet datasets with batch sizes ranging from 8 to 256 and can rebuild samples with greater similarity than the most recent approach. The research also introduces a label reconstruction algorithm that may improve upon the state-of-the-art technique by 27%, achieving a label reconstruction accuracy of 81% in a batch sample with a label repeat rate of 96%. The provided techniques may be used to evaluate the data security of FL systems for healthcare.

In the next work, Ahmed et al. [A12] proposed a technique for enhancing the effectiveness of deep neural networks (DNNs) in internet-delivered psychological treatment (IDPT) by expanding the accessibility of different and distinct training data. The suggested approach makes use of a structural hypergraph, an emotional lexicon, and an embedding model based on federated learning for the identification of mental health symptoms. According to experimental findings, the attention mechanism-equipped bidirectional LSTM architecture has a ROC of 0.86.

The use of IoMT devices in healthcare has led to privacy issues due to the centralized training approach of artificial intelligence (AI). FL is a distributive AI paradigm, can help preserve privacy in IoMT by allowing only gradients to be shared during training. Ali et al. [A13] discussed the use of FL in IoMT networks for privacy preservation and introduces advanced FL architectures incorporating deep reinforcement learning, digital twin, and generative adversarial networks. It also explores practical opportunities for FL in IoMT and discusses open research issues and challenges for using FL in future smart healthcare systems.

FL is a valuable approach in the medical field that allows for the collaborative training of machine learning (ML) models while keeping training data decentralized, thereby protecting privacy-sensitive medical data. However, FL is still unable to fully meet the stringent requirements of healthcare systems based on the IoMT. Aouedi et al. [A14] discussed the deployment of FL in the medical field, current approaches and challenges, and future directions for improving FL, particularly in terms of security and privacy.

Han et al. [A15] provided a FL-based zero-watermarking system to solve privacy and security challenges in teledermatology. Teledermatology uses smartphone photos for remote diagnosis, yet these images are subject to assaults. The proposed technique trains a sparse autoencoder network using federated learning to extract features from dermatological medical pictures, which are subsequently converted using 2D-DCT to pick low-frequency transform coefficients for constructing the zero-watermark. The approach outperforms existing zero-watermarking schemes in conventional and geometric assaults. The suggested technique is acceptable for medical photos since it protects crucial information and doesn't leak private data.

Tang et al. [A16] offered MRCG for safe and private MRI data retrieval in the IoMT (IoMT). MRCG combines CNN and GNN to graph gallery picture relationships. The system trains a Vgg16-based triplet network for similarity learning and classification, then uses a GNN with skip connections to learn on the graph and predict query and gallery picture similarity. MRCG beats other state-of-the-art models on benchmark datasets, attaining 88.64% and 86.59% mean Average Precision (mAP) on the CE-MRI and Kaggle datasets, respectively.

Samuel et al. [A17] proposed a privacy infrastructure based on FL and blockchain technology to address the limitations of current COVID-19 call centers, which may be overstressed and unable to provide adequate guidance due to high call volume and lack of data sharing between health institutions. The proposed infrastructure intends to improve public communication and disseminate COVID-19 information while addressing huge data silos and protecting data owners' privacy. Finally, the authors analyse and verify the security and privacy of the infrastructure.

Hossen et al. [A18] provided a skin disease classification system utilizing medical photos that combines CNN classification with FL to protect data privacy. The authors use image augmentation to enlarge a bespoke dataset with four skin disease types. The suggested CNN model performed well compared to benchmark algorithms for detecting skin disorders. The FL technique is applied to a dataset dispersed among several clients, resulting in an average accuracy of 81.21 percent, 86.57%, 91.15%, and 94.15%. The authors concluded that CNN-based skin disease categorization with FL ensures data confidentiality.

Han et al. [A19] provided a multi-source domain adaption technique for detecting medical disorders based on deep learning. It handles data heterogeneity and privacy protection in medical data sharing between institutions. The suggested solution aligns dispersed, heterogeneous data without transmitting source data, but rather pre-trained source models. This strategy protects patient privacy and saves network resources. The approach has a 69.37% accuracy on the ABIDE database. The authors also assess its resource-saving efficacy and generality.

In this research, Wang et al. [A20] proposed a privacy protection approach for FL in the context of edge computing, a sort of distributed machine learning that enables numerous devices or machines to jointly train a model without exchanging data. In addition to enhancing the effectiveness and real-time performance of edge intelligent computing, the plan safeguards the personal healthcare data in the IoMT. The suggested method is demonstrated to be quicker than differential privacy and more accurate and efficient than previous FL systems based on homomorphic encryption. It is built on secret sharing, weight masking, digital signatures, and hash functions. The system is ideal for usage in erratic edge computing contexts, such as smart healthcare, and is resistant to equipment dropping and collusion assaults amongst devices.

Sun et al. [A21] introduced SCALT, a scalable and portable classification method for HSD in edge computing and FL. SCALT uses a one-classifier-per-class technique with a one-dimensional convolutional network for feature extraction. It's designed to manage HSD's dynamic properties, such as changing data distributions and new classes, and to preserve patient privacy. SCALT protects against catastrophic parameter forgetting in sequential HSD classification jobs. The system outperforms state-of-the-art approaches on three physiological signal datasets, with accuracies of 98.65%, 91.10%, and 89.93% on the Electrocardiogram, Electroencephalogram, and Photoplethysmograph datasets, respectively.

Alamleh et al. [A22] proposed a multi-criteria decision-making (MCDM) framework for standardizing and measuring machine learning-based IDSs used in IoMT applications' FL architecture. The framework standardizes IDS assessment criteria using the fuzzy Delphi approach, formulates an evaluation decision matrix based on 125973 records and 41 attributes, and integrates MCDM methods to establish the important weights of security and performance criteria and pick the ideal IDSs. 14 out of 20 assessment criteria for security and 3 for performance obtained an agreement among experts. The BayesNet classifier is the best pick while SVM is the last. The area under curve criterion has the lowest weights while CPU time had the highest. IDSs is ranked, costed, and compared.

Ruby et al. [A23] studied the problem of client selection, channel allocation, and power control in the uplink process of federated learning (FL) in the IoMT domain in the presence of a malicious jammer robot. The interaction between the FL network and the jammer in each learning iteration is modeled as a Stackelberg game, with the jammer as the leader and the FL network as the follower. The joint best response strategy for both players is found using the difference of convex programming approach and the dual decomposition technique, and the problem is also considered from the perspective of partial information. Simulation results are presented to demonstrate the effectiveness of the proposed algorithms in the jamming game.

All the above papers tackle different but extremely relevant domain vectors of FL and blockchain for IoMT. We believe this Special Issue will raise awareness in the scientific community, through presenting and highlighting the advances and latest novel and emergent technologies, implementations, applications concerning the privacy preservation and security of the data generated from IoMT as well s optimize the communication cost and latency in IoMT. In closing, we would like to thank all the authors who submitted their research work to this special issue. We would also like to acknowledge the contribution of many experts in the field who have participated in the review process, and provided helpful suggestions to the authors to improve the contents and presentations of the articles. We would in particular like to thank Professor Dimitrios I. Fotiadis, the Editor-in-Chief, and the publishing team for their support and very helpful suggestions and comments during the delicate stages of concluding the special issue.

THIPPA REDDY GADEKALLU, *Guest Editor*
Vellore Institute of Technology
Vellore 632014, India

MAMOUN ALAZAB, *Guest Editor*
Charles Darwin University
Casuarina NT 0810, Australia

JUDE HEMANTH, *Guest Editor*
Karunya Uiversity
Coimbatore 641114, India

WEIZHENG WANG, *Guest Editor*
City University of Hong Kong
Hong Kong SAR
weizheng.wang@ieee.org

APPENDIX: RELATED ARTICLES

[A1] Z. Xu, Y. Guo, C. Chakraborty, Q. Hua, S. Chen, and K. Yu, "A simple federated learning-based scheme for security enhancement over Internet of Medical Things," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 652–663, 2023.

[A2] A. Lakhan et al., "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 664–672, 2023.

[A3] A. Lakhan et al., "Restricted Boltzmann machine assisted secure serverless edge system for Internet of Medical Things," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 673–683, 2023.

[A4] A. Rehman, I. Razzak, and G. Xu, "Federated learning for privacy preservation of healthcare data from smartphone-based side-channel attacks," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 684–690, 2023.

[A5] J. Ahmed, T. N. Nguyen, B. Ali, A. Javed, and J. Mirza, "On the physical layer security of federated learning based IoMT networks," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 691–697, 2023.

[A6] G. Xu et al., "A privacy-preserving medical data sharing scheme based on blockchain," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 698–709, 2023.

[A7] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 710–721, 2023.

[A8] P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, and A. Gurtov, "Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 722–731, 2023.

[A9] N. Wang, S. Zhang, Z. Zhang, J. Fu, J. Liu, and R. Wang, "Block-based privacy-preserving healthcare data ranked retrieval in encrypted cloud file systems," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 732–743, 2023.

[A10] A. S. Rachakonda et al., "Privacy enhancing and scalable federated learning to accelerate AI implementation in cross-silo and IoMT environments," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 744–755, 2023.

[A11] Z. Li, L. Wang, G. Chen, Z. Zhang, M. Shafiq, and Z. Gu, "E2EGI: End-to-end gradient inversion in federated learning," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 756–767, 2023.

[A12] U. Ahmed, J. C. W. Lin, and G. Srivastava, "Hypergraph attention based federated learning method for mental health detection," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 768–777, 2023.

[A13] M. Ali, F. Naeem, M. Tariq, and G. Kaddoum, "Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 778–789, 2023.

[A14] O. Aouedi, A. Sacco, K. Piamrat, and G. Marchetto, "Handling privacy-sensitive medical data with federated learning: Challenges and future directions," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 790–803, 2023.

[A15] B. Han, R. Jhaveri, H. Wang, D. Qiao, and J. Du, "Application of robust zero-watermarking scheme based on federated learning for securing the healthcare data," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 804–813, 2023.

[A16] Z. Tang, Z. H. Sun, E. Q. Wu, C. F. Wei, D. Ming, and S. Chen, "MRCG: A MRI retrieval system with convolutional and graph neural networks for secure and private IoMT," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 814–822, 2023.

[A17] O. Samuel et al., "IoMT: A COVID-19 healthcare system driven by federated learning and blockchain," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 823–834, 2023.

[A18] M. N. Hossen, V. Panneerselvam, D. Koundal, K. Ahmed, F. M. Bui, and S. M. Ibrahim, "Federated machine learning for detection of skin diseases and enhancement of Internet of Medical Things (IoMT) security," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 835–841, 2023.

[A19] T. Han, X. Gong, F. Feng, J. Zhang, Z. Sun, and Y. Zhang, "Privacy-preserving mutli-source domain adaptaion for medical data," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 842–853, 2023.

[A20] R. Wang, J. Lai, Z. Zhang, X. Li, P. Vijayakumar, and M. Karuppiah, "Privacy-preserving federated learning for Internet of Medical Things under edge computing," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 854–865, 2023.

[A21] L. Sun and J. Wu, "A scalable and transferable federated learning system for classifying healthcare sensor data," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 866–877, 2023.

[A22] A. Alamleh et al., "Federated learning for IoMT applications: A standardisation and benchmarking framework of intrusion detection systems," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 878–887, 2023.

[A23] R. Ruby, H. Yang, and K. Wu, "Anti-jamming strategies for federated learning Internet of Medical Things: A game approach," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 888–899, 2023.

References

[1] S. P. RM et al., "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, 2020.

[2] M. Alazab, S. P. RM, P. K. R. Maddikunta, T. R. Gadekallu, and Q. V. Pham, "Federated learning for cybersecurity: Concepts, challenges, and future directions," *IEEE Trans. Ind. Inform.*, vol. 18, no. 5, pp. 3501–3509, May 2022.

[3] Z. Lian, Q. Zheng, W. Wang, T. R. Gadekallu, C. Su, and P. Yadav, "Blockchain-based two-stage federated learing with non-IID data in IoMT system," *IEEE Trans. Comput. Social Syst.*, early access, Nov. 21, 2022.

[4] J. Song, W. Wang, T. R. Wang, T. R. Gadekallu, J. Cao, and Y. Liu "EP-PDA: An efficient privacy-preserving data aggregation federated learning scheme," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 25, 2022.

[5] Z. Lian et al., "DEEP-FEL: Decentralized, efficient and privacy-enhanced federated edge learning for healthcare cyber physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 3558–3569, Sep./Oct. 2022.

[6] W. Wang et al., "Secure-enhanced federated learning for AI-empowered electric vehicle energy prediction," *IEEE Consum. Electron. Mag.*, vol. 9, early access, Sep. 30, 2021.

[7] K. S. Arikumar et al., "FL-PMI: Federated learning-based person movement identification through wearable devices in smart healthcare systems," *Sensors*, vol. 22, no. 4, 2022, Art. no. 1377.