IEEE JOURNAL OF

BIOMEDICAL AND HEALTH INFORMATICS

J-BHI Special Issue on "Privacy-Preserving Cloud Computing with Federated Learning for Healthcare Data"

The early identification of illnesses is becoming more accessible and reasonably priced because of the smart healthcare system's quick development. Nonetheless, the primary cause of anxiety is the computer's possible major confidentiality risk. Due to the scattered nature of healthcare data as well as its rapid expansion, industrial cloud computing and the growing Internet of Things have completely changed the healthcare sector. The perfect guarantee of the safety of healthcare data cannot be achieved with the current privacy-preserving measures. Rather than being subject to a beyond assault, the majority of healthcare data stored on cloud servers is under attack from within. Among the most important issues facing the healthcare sector are the security and privacy of patient data. Convolutional neural networks were used to classify normal and deviant users from the analysed information. The aberrant users were subsequently evaluated and eliminated from the repository, in addition to the availability of the health information, according to the integration of blockchain technology with a federated learning mechanism that employs secrecy.

Federated learning serves as a unique artificial intelligence method that protects privacy while providing contextual information about data in smart cities. In order to preserve privacy in intelligent healthcare, a secure architecture supported by federated learning and digital currency technology is needed. Cryptocurrency-based cloud services for IoT are utilised to ensure confidentiality and safety. Affordable gadget-acquiring applications, such as those in healthcare, use supervised learning systems. One of the main issues with healthcare data is security and privacy. Safeguarding private information is a common definition of privacy. The growing volume of medical data that is becoming a crucial component of patient treatment is the cause of the assault on medical information. Exterior antagonists are usually prevented by identification and encryption mechanisms, but inner hostile activity is the main problem since it leads to assaults like recollect and interruption of service attacks, among others. Furthermore, as medical data involves important data regarding patients, secrecy is a critical concept in the therapeutic system. FL is a decentralised method that gives several network nodes individualised, resilient, and privacy-aware data. It offers enhanced privacy protection and efficiency in a variety of software, making it very promising. This special issue addresses the latest developments in federated learning to tackle this issue within the framework of computation that protects privacy. Federated learning offers significant advantages to healthcare systems, excellent protection and privacy assurances, and the ability to develop and employ global AI models across numerous decentralised data sources. The origins, goals, explanations, platforms, and potential uses of federated learning are presented in this special issue as an alternative model for creating trustworthy, privacy-preserving AI societies.
Topics of interest include, but are not limited to, the following:

- A smart medical system powered by federated learning and protects privacy
- Cloud computing-based federated learning for privacy-preserving Web of medical things
- Federated learning as an architecture for Smart healthcare dataset privacy preservation
- Regarding healthcare data networks, a privacy-preserving federated learning architecture
- IoT-enabled medical facilities using homomorphic safeguarding for privacy-preserving federated learning
- Collaborative learning and a reliable, privacy-preserving modular ensembles in healthcare
- A structure protects privacy for federated learning in intelligent health systems
- A federated learning-based privacy-preserving cloud computing platform for managing health
- Federated learning-based cloud computing with privacy preservation for intelligent utilities
- Implementing Federated Machine Learning to Leverage Privacy Preservation for Health Care Facilities
- A secure and private federated learning application platform for Internet of Things

Guest Editors

Dr. Adnan Shahid Khan - Universiti Malaysia Sarawak (UNIMAS), Kota Samarahan, Malaysia, adnanskhan084@gmail.com
Dr. Irshad Ahmed Abbasi - University of Bisha, Bisha, Saudi Arabia, aabasy@ub.edu.sa
Dr. Kashif Nisar - Swinburne University of Technology, Sydney, New South Wales, Australia, knisar@swin.edu.au

Key Dates

Deadline for Submission: 01 Nov, 2024
First Reviews Due: 01 Jan, 2025
Revised Manuscript Due: 01 Mar, 2025
Final Decision: 01 May, 2025