RADemics

Federated Learning and Data Privacy in Connected Healthcare Devices

A. Thanikasalam, S Bharathi, Amit Kumar Bhakta
ACADEMY OF MARITIME EDUCATION AND TRAINING, DEEMED TO BE UNIVERSITY, SETHU INSTITUTE OF TECHNOLOGY, SEACOM ENGINEERING COLLEGE

Federated Learning and Data Privacy in Connected Healthcare Devices

[1]A. Thanikasalam, Assistant Professor, Department of Marine Engineering, Academy of Maritime Education and Training, Deemed to be University, 135 East Coast Road, Kanathur – 603112. thanikasalama@ametuniv.ac.in

[2]S Bharathi, Assistant Professor, Department of Civil Engineering, Sethu Institute of Technology, Pulloor, Kariapatti – 626115. bharathysanthanam@sethu.ac.in

[3]Amit Kumar Bhakta, Associate Professor, Department of Mechanical Engineering, Seacom Engineering College, Howrah -711302. akbiit41@gmail.com

Abstract

Federated learning has emerged as a transformative paradigm for secure and intelligent healthcare systems, enabling collaborative model training without centralized data aggregation. This book chapter explores the architectural foundations, privacy-preserving techniques, and real-world applications of federated learning in connected healthcare environments. The discussion emphasizes the integration of decentralized artificial intelligence with Internet of Medical Things (IoMT) devices, facilitating clinical decision support, real-time health prediction, and continuous patient monitoring while maintaining strict compliance with data protection regulations. The chapter examines communication frameworks, model update mechanisms, and scalable system architectures that ensure interoperability across diverse healthcare infrastructures. Security challenges such as data poisoning, inference attacks, and model inversion are analyzed in conjunction with robust defense mechanisms including differential privacy, secure multi-party computation, and homomorphic encryption. Through an in-depth examination of federated learning's role in privacy-preserving analytics, this work highlights its potential to revolutionize precision medicine, telehealth, and patient-centric digital ecosystems. The synthesis of distributed intelligence and ethical AI practices positions federated learning as a cornerstone technology for the future of connected and trustworthy healthcare innovation.

Keywords: Federated Learning, Connected Healthcare, Data Privacy, Clinical Decision Support, Real-Time Health Prediction, Secure Aggregation.

Introduction

The emergence of federated learning has redefined the technological foundations of digital healthcare by providing a secure and collaborative framework for artificial intelligence development [1]. Traditional centralized machine learning systems, though effective in large-scale data analysis, present significant challenges related to patient privacy, data ownership, and institutional data sharing restrictions [2]. In healthcare, where data confidentiality and ethical responsibility are paramount, federated learning enables a paradigm shift by training models locally on decentralized datasets without transferring raw information to a central server [3]. This approach eliminates the risk of data leakage and aligns with global data protection regulations,

creating a secure foundation for intelligent health analytics [4]. By uniting hospitals, diagnostic laboratories, and connected devices under a single collaborative ecosystem, federated learning accelerates the advancement of precision medicine while maintaining the integrity and confidentiality of sensitive health records. This evolution in data governance not only enhances trust but also expands the potential for innovation in clinical decision-making and predictive healthcare systems [5].

The connected healthcare environment has evolved into a vast network of devices, sensors, and digital platforms that continuously collect and analyze patient data for preventive, diagnostic, and therapeutic purposes [6]. The integration of federated learning into this ecosystem addresses long-standing challenges related to interoperability, scalability, and data security [7]. Connected medical devices such as wearable sensors, implantable monitors, and smart hospital systems produce heterogeneous datasets that are often fragmented and isolated across institutions [8]. Federated learning bridges this fragmentation by enabling collaborative model development across distributed data sources, ensuring that valuable medical insights are not limited to individual repositories [9]. Through decentralized computation, the technology supports real-time learning across multiple nodes, enhancing diagnostic precision, and enabling adaptive health monitoring systems. This dynamic collaboration empowers healthcare providers to harness diverse medical datasets while maintaining compliance with ethical and legal standards governing patient data protection [10].

The architecture of federated learning in healthcare is designed to accommodate the unique constraints of distributed medical systems [11]. Each participant within the network operates as a local computing node that processes and trains data independently while communicating model parameters to a central aggregator [12]. This iterative process of training and aggregation facilitates continuous model improvement while safeguarding data privacy [13]. The architectural design typically includes three layers local device intelligence, secure communication protocols, and global model coordination to maintain seamless interaction among all components of the healthcare network. This structure ensures robust data integrity, resilience against cyberattacks, and efficient model synchronization [14]. Scalability remains a defining feature of this architecture, enabling it to support thousands of devices simultaneously without overloading network resources. In the healthcare context, this design allows hospitals, research centers, and mobile health systems to collaborate in real-time, creating unified diagnostic frameworks that improve clinical efficiency and patient care outcomes [15].