RADemics

Integration of Federated Learning in Decentralized Healthcare Networks for Urban Health Monitoring

Syeda Sadia Tabassum , P. Malar
Visvesvaraya Technological University, Velalar College of Engineering and Technology

6. Integration of Federated Learning in Decentralized Healthcare Networks for Urban Health Monitoring

[1]Syeda Sadia Tabassum, Assistant Professor, Department of Computer Science and Engineering, HKBK College of Engineering, Visvesvaraya Technological University, Bangalore 560045, Karnataka, India, syeda92sadia@gmail.com

[2]P. Malar, Assistant Professor, Department of Information Technology, Velalar College of Engineering and Technology, Thindal, Erode-638012, India, malar.prof24@gmail.com.

Abstract

Federated Learning (FL) has emerged as a promising solution for privacy-preserving collaborative machine learning in decentralized networks, particularly within healthcare systems. This book chapter explores the integration of FL in urban health monitoring, emphasizing the critical role of privacy-preserving techniques to mitigate risks associated with sensitive health data. With the increasing adoption of decentralized healthcare networks, privacy concerns related to data sharing and model updates have become paramount. This chapter addresses key privacy threats in Federated Learning, such as adversarial attacks, data leakage, and malicious model manipulation, while proposing robust mitigation strategies. The application of differential privacy, secure aggregation protocols, and anonymization techniques was discussed, alongside their challenges in maintaining model accuracy and performance. Additionally, the chapter highlights the trade-off between privacy preservation and computational overhead, underscoring the need for efficient solutions that balance both. Through a comprehensive analysis, this chapter offers insights into the future of Federated Learning in healthcare, advocating for stronger privacy guarantees, secure collaboration, and the advancement of machine learning models to enable effective urban health monitoring.

Keywords: Federated Learning, Privacy-Preserving Techniques, Healthcare Networks, Differential Privacy, Secure Aggregation, Urban Health Monitoring.

Introduction

Federated Learning (FL) has become a pivotal framework in modern machine learning, particularly in healthcare, due to its ability to preserve data privacy while enabling collaborative model development [1]. As healthcare systems transition to decentralized models, FL provides a solution that allows different institutions, devices, and users to collaboratively train models without the need to share sensitive data [2]. This was crucial in healthcare, where patient data privacy was a legal and ethical necessity [3]. The rise of urban health monitoring systems, which collect and analyze health data from multiple urban sources such as hospitals, wearable devices, and public health organizations, highlights the need for privacy-preserving technologies like FL

[4]. while FL offers significant privacy benefits, it also brings challenges regarding the security of data during model training and the potential for adversarial attacks [5].

One of the fundamental challenges associated with Federated Learning in healthcare was ensuring the confidentiality of sensitive patient information [6]. In a typical centralized machine learning setting, data was collected and stored in a single location, making it vulnerable to data breaches [7]. FL eliminates the need for such centralized data storage, allowing data to remain on local devices or servers while only model updates are shared [8]. This approach significantly reduces the risk of exposing sensitive information [9]. even with local data storage, there are still risks associated with the exchange of model parameters, which could potentially reveal private insights about individual patients [10]. To address this, advanced privacy-preserving techniques, such as differential privacy and secure aggregation protocols, must be employed to ensure that the privacy of health data was maintained throughout the learning process [11].

The integration of Federated Learning in decentralized healthcare networks also faces substantial hurdles in terms of computational complexity and system efficiency [12]. While FL offers privacy benefits, it requires frequent model updates to be sent between different participating nodes, which can result in high communication costs and substantial computational overhead [13]. This can be particularly problematic in healthcare settings where the systemsbe constrained by limited computational resources or slow internet connections [14]. Ensuring that the models developed in such a decentralized environment retain their accuracy and effectiveness in real-world applications was a significant challenge [15]. Balancing privacy preservation with system efficiency becomes critical, especially in large-scale urban health monitoring systems that need to process vast amounts of data from diverse sources without compromising performance [16].

An additional consideration in Federated Learning within healthcare systems was the risk posed by adversarial attacks [17]. In a decentralized setup, malicious participants or compromised devicesattempt to manipulate model updates with the intent of sabotaging the learning process [18]. Such attacks could compromise the accuracy of the trained model or even manipulate it to produce biased or harmful outcomes, posing a significant risk to patient health and safety [19]. To mitigate this, advanced techniques such as anomaly detection and secure aggregation protocols have been proposed [20]. These methods aim to identify and eliminate malicious updates beforeaffect the overall model, ensuring that the federated model remains robust and secure even in the presence of adversaries [21]. there was a continual need to evolve these defense mechanisms, as adversariesadapt their strategies over time.

While Federated Learning presents a transformative opportunity for urban health monitoring, its successful implementation depends on the development of solutions that address both privacy concerns and operational challenges [22]. The ability to share and analyze data across multiple decentralized entities while preserving individual privacy was essential for building trust in Federated Learning systems [23]. This aims to explore the intersection of privacy-preserving techniques and Federated Learning in healthcare, outlining the current state of research and identifying key challenges [24]. The detailed examination of existing solutions, including differential privacy, secure aggregation, and data minimization strategies, to support the development of secure and privacy-preserving federated models in healthcare [25].