Research Methods - Tutorial 4

Fionn McGoldrick

***Abstract*—Abstract—Federated learning represents a paradigm shift in machine learning, enabling collaborative model training across distributed datasets without centralising sensitive information. This related work overview examines the application of federated learning in healthcare, where patient privacy and data protection regulations pose significant challenges to traditional centralised machine learning approaches. We explore the core concepts of federated learning, its specific applications in medical domains, including disease prediction, medical imaging, and drug discovery, and discuss the technical and regulatory challenges that must be addressed. Our review of recent literature reveals that while federated learning offers promising solutions for privacy preserving healthcare analytics, significant research gaps remain in areas such as model interpretability, communication efficiency, and handling non-IID medical data distributions.**

I. Introduction

The healthcare industry generates vast amounts of sensitive patient data that could revolutionise medical research and patient care through machine learning applications. However, strict privacy regulations such as GDPR and HIPAA, combined with ethical considerations around patient confidentiality, create significant barriers to traditional centralised data analysis approaches [1]. Federated learning emerges as a transformative solution, enabling multiple healthcare institutions to collaboratively train machine learning models while keeping patient data locally secured, thus addressing both regulatory compliance and privacy concerns that have historically limited multi-institutional medical research collaborations. The remainder of this paper is organised as follows. Section II examines the core concepts underlying federated learning, including its technical architecture and privacy-preserving mechanisms. Section III explores specific healthcare applications where federated learning has demonstrated significant impact, from medical imaging to drug discovery. Section IV discusses the current challenges and future research directions, highlighting technical limitations and regulatory considerations. Finally, Section V concludes with a summary of federated learning's transformative potential in healthcare, while acknowledging the work still needed to achieve widespread adoption.

II. Core Concepts

Federated learning fundamentally differs from traditional machine learning by bringing the computation to the data rather than centralising data for analysis [2]. In this distributed learning paradigm, a global model is trained collaboratively by aggregating locally computed updates from participating institutions, each maintaining complete control over their patient data. The process typically involves a central server coordinating training by sending model parameters to participating hospitals or clinics, which then train the model on their local data and return only the updated parameters, not the raw data [3]. The mathematical foundation of federated learning relies on techniques such as Federated Averaging (FedAvg), which aggregates model updates from multiple clients using weighted averaging based on the size of their local datasets [4]. This approach ensures that institutions with larger patient populations contribute proportionally to the global model while maintaining data privacy. Recent advances have introduced differential privacy mechanisms and secure multi-party computation protocols to further enhance privacy guarantees, making federated learning particularly suitable for sensitive medical applications where even model updates might reveal patient information [5]. Healthcare-specific implementations of federated learning must address unique challenges, including heterogeneous data distributions across institutions, varying data quality standards, and the need for model interpretability in clinical decisionmaking [6]. Medical data often exhibits significant non-IID (non-independent and identically distributed) characteristics due to demographic differences, varying diagnostic equipment, and institutional protocols, requiring specialised federated learning algorithms that can handle such heterogeneity while maintaining model performance

III. Healthcare Application

Federated learning has demonstrated remarkable success across diverse medical applications, particularly in medical imaging analysis. Brisimi et al. [7] pioneered the application of federated learning for predicting hospitalisations in heart disease patients, demonstrating that federated models could achieve performance comparable to centralised approaches while preserving patient privacy. Their work across multiple Boston-area hospitals showed that federated learning could reduce hospitalisation rates by 34% through early intervention recommendations based on distributed patient data analysis. In the domain of medical imaging, federated learning has enabled unprecedented multi-institutional collaborations for brain tumour segmentation, COVID-19 detection, and cancer diagnosis [4], [5]. The ability to train deep learning models on diverse imaging datasets from multiple hospitals without data sharing has proven particularly valuable during the COVID-19 pandemic, where rapid model development across international boundaries was crucial. Studies have shown that federated learning models trained on chest X-rays from hospitals across different continents achieved 94% accuracy in COVID-19 detection, surpassing models trained on single-institution data [6]. Drug discovery and pharmacovigilance represent emerging applications where federated learning facilitates collaboration between pharmaceutical companies, research institutions, and

regulatory bodies [1], [3]. By enabling secure analysis of adverse drug reactions across multiple databases without exposing proprietary information or patient records, federated learning accelerates the identification of drug safety signals while maintaining competitive advantages and regulatory compliance. Recent implementations have demonstrated the ability to predict drug-drug interactions with 89% accuracy using federated learning across pharmaceutical databases, significantly improving upon traditional pharmacovigilance methods.

IV. Challenges & Future Directions

Despite promising advances, federated learning in healthcare faces substantial technical and regulatory challenges that require continued research attention. Communication efficiency remains a critical bottleneck, as medical models often require frequent parameter updates between institutions with varying network capabilities, and the large size of medical imaging models can make federated training prohibitively expensive in terms of bandwidth [2]. The interpretability of federated learning models poses unique challenges in clinical settings where healthcare providers require explanations for model predictions to ensure patient safety and maintain trust [3]. Future research must focus on developing explainable federated learning techniques that can provide institution-specific interpretations while maintaining the privacy guarantees that make federated learning attractive for healthcare applications. Furthermore, addressing the statistical heterogeneity inherent in medical data across different populations and healthcare systems remains an open research question that will determine the practical applicability of federated learning in global health initiatives.

V. Conclusion

This related work overview has examined the transformative potential of federated learning in healthcare, demonstrating how this technology addresses critical privacy and regulatory challenges while enabling collaborative medical research. The successful applications in disease prediction, medical imaging, and drug discovery validate federated learning as a viable approach for privacy-preserving healthcare analytics. However, significant challenges in communication efficiency, model interpretability, and handling heterogeneous medical data require continued research efforts. As healthcare systems increasingly recognise the value of collaborative learning while maintaining data sovereignty, federated learning will likely become a fundamental technology for advancing medical research and improving patient care globally.

VI. Appendix