A Comprehensive Survey of Privacy-preserving Federated Learning: A Taxonomy, Review, and Future Directions

XUEFEI YIN, School of Engineering and Information Technology, University of New South Wales
YANMING ZHU, School of Computer Science and Engineering, University of New South Wales
JIANKUN HU, School of Engineering and Information Technology, University of New South Wales

The past four years have witnessed the rapid development of federated learning (FL). However, new privacy concerns have also emerged during the aggregation of the distributed intermediate results. The emerging privacy-preserving FL (PPFL) has been heralded as a solution to generic privacy-preserving machine learning. However, the challenge of protecting data privacy while maintaining the data utility through machine learning still remains. In this article, we present a comprehensive and systematic survey on the PPFL based on our proposed 5W-scenario-based taxonomy. We analyze the privacy leakage risks in the FL from five aspects, summarize existing methods, and identify future research directions.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Computing methodologies** → **Machine learning**; • **Security and privacy** → **Privacy-preserving protocols;**

Additional Key Words and Phrases: Privacy-preserving federated learning, data privacy, horizontal federated learning, vertical federated learning, federated transfer learning, cryptographic encryption, perturbation techniques, anonymization techniques

ACM Reference format:
Xuefei Yin, Yanming Zhu, and Jiankun Hu. 2021. A Comprehensive Survey of Privacy-preserving Federated Learning: A Taxonomy, Review, and Future Directions. *ACM Comput. Surv.* 54, 6, Article 131 (July 2021), 36 pages.
https://doi.org/10.1145/3460427

1 INTRODUCTION

1.1 Background

The concept of **federated learning (FL)** was first introduced in 2016 [121]. Its core idea is to train machine learning models on separate datasets that are distributed across different devices or parties, which can preserve the local data privacy to a certain extent. Since then, FL has achieved a rapid development and become a hot research topic in the field of artificial intelligence [9, 131]. The

This research is supported by ARC Discovery Grant with project ID DP190103660, DP200103207 and ARC Linkage Grant with project ID LP180100663.
Authors' addresses: X. Yin and J. Hu (corresponding author), School of Engineering and Information Technology, University of New South Wales, Northcott Drive, Canberra, ACT, Australia, 2602; emails: xuefei.yin@unsw.edu.au, J.Hu@adfa.edu.au; Y. Zhu, School of Computer Science and Engineering, University of New South Wales, Anzac Parade, Sydney, NSW, Australia, 2052; email: yanming.zhu@unsw.edu.au.

0360-0300/2021/07-ART131 $15.00
https://doi.org/10.1145/3460427