1) Federated Machine Learning : Concept & Applications (Jan 2019)

10.1145/3298981

Federated Machine Learning, introduced by Google in 2016, is a ML technique, that trains an algorithm across multiple decentralized edge devices or servers holding local data samples without exchanging them. F.L enables multiple devices to build a common, robust ML model without sharing data, solving issues like data-privacy, data-security, data-access rights & heterogeneous data.

This paper is based on the concept of secure Federated Learning. It talks about the various concepts of security in FL like

- Secure Multiparty Computation (SMC)
- Differential Privacy
- Homomorphic Encryption
- Indirect Information Leakage

Next, we have the categories of F.L

- Horizontal F.L
- Vertical F.L
- Federated Transfer Learning

The paper also discusses the basic implementation & theoretical aspects of these usecases of F.L

The next section describes the various applications of F.L