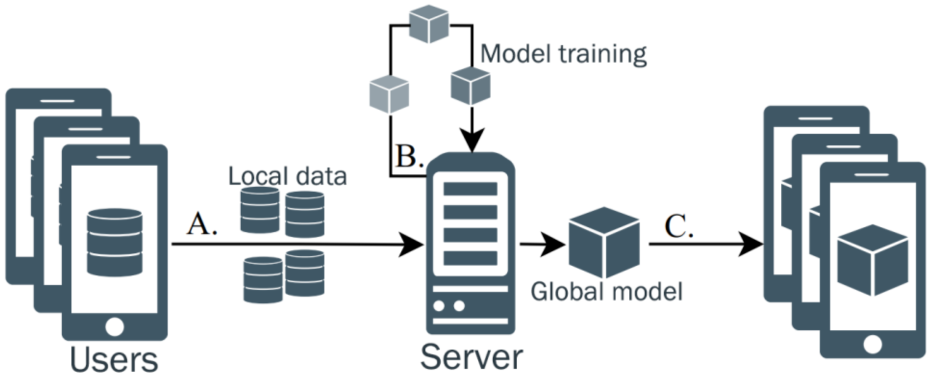
Challenges and Future Directions of Secure Federated Learning: A Survey

Kaiyue ZHANG, Xuan SONG, Chenhan ZHANG, Shui YU

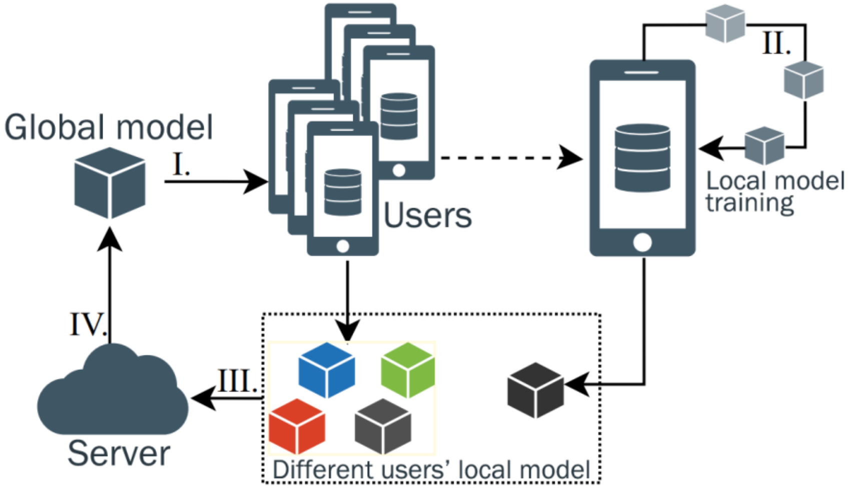
Frontiers of Computer Science, DOI: 10.1007/s11704-021-0598-z

Background & Introduction

- Federated learning came into being with the increasing concern of privacy security of traditional deep learning.
- Nevertheless, though existing federated learning applications are diverse and successful, it still faces many challenges.



Traditional deep learning



Federated learning

Main Contributions

- We discussed five challenges that future federated learning systems worth to be focused on:
  - Communication cost
  - Systems heterogeneity
  - Statistical heterogeneity
  - Privacy concern
  - Other vulnerabilities

- We pointed out three promising future directions of federated learning:
  - Privacy and security protection
  - Incentive mechanism for federated learning
  - Personalized federated learning