Differentially Private Federated Machine Learning For Large Models And A Strong Adversary

Tech ID: 33272 / UC Case 2023-867-0

BACKGROUND

Systems that preserve digital user privacy are essential, especially with the emergence of new privacy regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act. Large investments in this field from high-profile digital giants reinforce the need for novel privacy technologies. Due to the scientific and economic value of user data, a secure exchange from one party to another is necessary, and this exchange has inspired two novel concepts: federated averaging (FedAvg) and differential privacy (DP). When combined, FedAvg and DP offer a decentralized and secure mode of extracting and exchanging key info from large datasets. However, current systems that employ these two concepts are vulnerable to malicious devices and require substantial computational resources from edge devices.

DESCRIPTION

Researchers at the University of California, Santa Barbara, have developed a software system that allows differentially-private federated machine learning over confidential data stored on mobile devices in a privacy-safe manner. The system uses stochastic federated averaging (FedAvg) to free devices from generating gradients in all rounds, such that part of proof generation can be completed offline before the round(s) in which it participates. Splitting ZK-proof generation across rounds and optimizing the verification of ciphertext sums further enhances the system and reduces overall model training time. The system is built on a framework that guarantees central differential privacy (CDP), ensuring cutting-edge security of user data. This technology is optimized for performance and scalability to a large number of mobile devices and models with a large number of parameters.

ADVANTAGES

- Trains machine learning models while ensuring the privacy of training data
- Reduces overall system training time
- Reduces requirement for computational resources on edge devices

APPLICATIONS

- Software

CONTACT

Pasquale S. Ferrari
ferrari@tia.ucsb.edu
tel: .

INVENTORS

- Gupta, Trinabh
- Liu, Kunlong
- Wadaskar, Richa

OTHER INFORMATION

KEYWORDS

Differentially private federated learning, Machine learning privacy, Confidential data, Federated averaging, Differential privacy, Mobile devices, Central differential privacy, Strong adversary

CATEGORIZED AS

- **Computer**
  - Security
  - Software

RELATED CASES

2023-867-0

- Security
- Privacy

RELATED MATERIALS

▶ Towards an Efficient System for Differentially-private, Cross-device Federated Learning - 10/25/2021