Differential Privacy for Deep and Federated Learning: A Survey 2022

IEEE ACCESS: AHMED EL OUADRHIRI AND AHMED ABDELHADI, (Senior Member, IEEE)

Contributions

1. A comprehensive description of the probability distributions that satisfy the ε-DP definition with their use cases.
2. A detailed description of ε-DP variants, namely (ε, δ)-DP, (α, ε)-rényi DP, and f-DP, comparing the privacy leakage due to composition..
3. A review of the different works based on DP for protecting users' privacy in DL and FL. We divide these approaches into three categories based on their type of application: 1) PP queries, 2) PP datasets, 3) PP models.
4. An analysis of the main ideas and recent approaches based on DP regarding the computational complexity, communication cost, and accuracy. This analysis illustrates the gap between theory, application, accuracy, and robustness of DP and brings forth many future research directions.

- The main objective of DP is allow studying the properties of a dataset as a whole without revealing one's individual privacy information.

- Author propose Fourier Summation Algorithm (FSA), combines the private summation protocol with the Discrete Fourier Transform (DFT) from Rastogi and Nath in the centralized case, to improve the accuracy of the tight bound to $O_{\varepsilon,\delta}(m^{8/3}n^{-5/3})$, where m represents the number of Fourier coefficients retained.

- Ultimately, the RDP allows determining a tighter bound, of the privacy leakage due to composition, compared to the start-of-the-art privacy bounds calculated using the original definition of (ε, δ)-DP

Method

- Central differential privacy for Deep learning

  (1) There are three categories of works in the literature: The first category consists of predefining an acceptable accuracy c and then determines the optimal privacy leakage ε that guarantees the highest privacy protection and an accuracy greater than the predefined accuracy c. The second category consists of predefining the privacy leakage that should be guaranteed and then determining the learning model parameters the maximize the accuracy . The third category consists of adding noise based on the relevance of each input feature to the outputs.
  (2) PRIVACY-PRESERVING LEARNING MODEL
  (3) PRIVACY-PRESERVING QUERY RESULTS.
  (4) PRIVACY-PRESERVING DATASETS

Probability distribution	Noise	Use cases	Privacy leakage
Laplace [29]	Adds real values drawn from $Lap(0, \frac{\Delta_f}{\epsilon})$.	Protects queries' results, datasets, gradients.	ϵ-DP
Gaussian [54]	Adds real values drawn from $\mathcal{N}(0, \frac{\Delta_f^2}{\epsilon^2})$.	Protects queries' results, datasets, gradients.	(ϵ, δ)-DP
Geometric [55]	Adds a discrete value δ with probability $P(\Delta = \delta) = \frac{1-e^{-\epsilon}}{1+e^{-\epsilon}} e^{-\epsilon\|\delta\|}$.	Protects queries' results, datasets.	ϵ-DP
Exponential [58]	Chooses a random output with probability $e^{(\frac{\epsilon u(D,y)}{2\Delta u})}$.	Protects learning models.	ϵ-DP
Binomial [59]	Adds discrete value drawn from $(Bin(N,p) - Np)s$.	Protects queries' results, datasets.	(ϵ, δ)-DP

- LOCAL DIFFERENTIAL PRIVACY FOR DEEP LEARNING

(1) In the first step, each client splits the weights of their local model, but labels each weight with an id to indicate its location of the weight in the network structure.
(2) In the second step, each client samples a small random latency t from a uniform distribution $U(0,T)$, where $T > 0$, for each weight and waits for t before sending the weight to the cloud.

Ref.	Year	DP-mechanism	Main contribution	Objective
[111]	2021	Gaussian	Approach for efficient hierarchical caching in fog computing. The authors use FL for collaborative training and DP to protect the IoT devices' privacy.	Protecting the privacy of IoT devices while training an FL model for content popularity prediction.
[112]	2021	Gaussian	Functional encryption mechanism to secure the communication between the clients and the server. The privacy of clients is protected using DP.	PP model while ensuring the privacy of clients during the training process.
[34]	2021	Gaussian	A new PP approach that consists of only sharing partial parameters of the client's gradient with the server. The authors introduce a proxy server between the clients and the server to ensure the anonymity of the gradients.	PP model while ensuring the privacy of clients during the training process.
[113]	2021	Gaussian	Determining the standard deviation of the Gaussian distribution to achieve a predefined privacy leakage after T synchronization rounds. Proposing an algorithm for adjusting T to get the best convergence performance.	PP model while ensuring the privacy of clients during the training process.
[31]	2021	Gaussian	Decentralized learning by a token τ transiting in the network via peer-to-peer communication. The token is updated sequentially by each device before sending it to another device.	PP model while ensuring the privacy of clients during the training process.
[32]	2021	Gaussian	Characterize the Gaussian noise variance σ^2 required to guarantee a target privacy budget ϵ after T synchronization rounds.	Protecting the clients' privacy during the training and reducing the communication overhead.
[84]	2020	Laplace	Formalize an optimization problem subject to communication overheard, accuracy, and privacy budget.	Protecting the clients' privacy during the training and reducing the communication overhead.
[114]	2020	Gaussian	Asynchronous FL model with LDP to reduce the communication overhead and a mechanism to detect malicious nodes.	Protecting the clients' privacy during the training and reducing the communication overhead.
[115]	2020	Binomial	Formalize an optimization problem to determine the transmission rates allocation for the clients with regards to the privacy budget and the communication constraints.	Protecting the clients' privacy during the training and reducing the communication overhead.
[116]	2020	Gaussian	Apply DP in federated multi-task learning to protect the clients' privacy. The multi-task learning is used to deal with heterogeneous datasets.	Protecting the privacy of clients participating in federated multi-task learning.
[117]	2020	Randomized response	Approach to protect the privacy of clients while training a DL model with a cloud server. The first layers of the DL model are located at the clients with a new layer called LATENT to protect the privacy, and the last layers are located at the cloud server.	Protecting the clients' privacy while collaboratively training a DL model.
[118]	2020	Laplace	Framework to protect the privacy of clients participating in an FL model using DP and homomorphic encryption.	Protecting the privacy of clients while training an FL model.
[119]	2021	Uniform, Laplace, Gaussian	Framework called SDTF to protect the privacy of clients while training an FL model without a server. The privacy is protected using DP and Elgamal cryptosystem.	Protecting the privacy of clients while training a decentralized FL model.
[120]	2021	Random noise	Framework called chain-PPFL to protect the privacy of clients in an FL network using secure multiparty computing.	Protecting the privacy of clients while training a decentralized FL model.