METHODS, APPARATUSES, AND SYSTEMS FOR MULTI-PARTY COLLABORATIVE MODEL UPDATING FOR PRIVACY PROTECTION

ABSTRACT

Embodiments of this specification provide a method and an apparatus for multi-party collaborative model updating for privacy protection. In a collaborative model updating method, each participant i determines a corresponding local gradient vector based on a local sample set and current model parameters, and performs random binarization processing on elements in the local gradient vector by using a randomized algorithm that satisfies differential privacy, to obtain a perturbed gradient vector. Each participant i sends the determined perturbed gradient vector to a server. The server aggregates n perturbed gradient vectors, and performs binary representation on elements in a current aggregation result based on plus-minus signs of the elements, to obtain a target gradient vector. Each participant i receives the target gradient vector from the server, and updates the current model parameters based on the target gradient vector for a next round of iteration. After a plurality of rounds of iterations, each participant i uses the current model parameters obtained by the participant i as a service prediction model that is updated by the participant i in collaboration with other participants.

FIG. 4