

DATA PRIVACY PROTECTION MULTI-PARTY JOINT TRAINING METHOD AND APPARATUS

ABSTRACT

Embodiments of this specification provide a data privacy protection multi-party joint training
5 method and apparatus, where a plurality of parties respectively hold different feature parts of a
shared sample; and the method is applied to a label party that further holds a sample label in the
plurality of parties, and includes: processing the shared sample by using a local first embedding
model, to obtain a first embedding vector; processing, by using a local first prediction model, a
fusion vector between the first embedding vector and embedding vectors provided by the other
10 parties for the shared sample, to obtain a first prediction result, and determining a first training loss
in combination with the sample label; processing the shared sample by using a local second
embedding model and a local second prediction model, to obtain a second prediction result, and
determining a second training loss in combination with the sample label; and determining, by using
an embedding vector output by an embedding model corresponding to a smaller value in the two
15 training losses as a label, a third training loss of the other embedding model for the shared sample,
where the determined training losses are used to train models respectively locally deployed by the
plurality of parties.

FIG. 3

20