

FEDERATED LEARNING METHODS AND APPARATUSES, READABLE STORAGE MEDIA, AND ELECTRONIC DEVICES

ABSTRACT

This application relates to federated learning methods and apparatuses, readable storage media, and electronic devices. The method includes the following: a first aspect program is injected at a gradient sending function of a federated learning device by using a pre-deployed aspect framework; a to-be-trained model is trained based on local training data to obtain a plaintext gradient of the to-be-trained model, and the plaintext gradient is sent to a federated learning server by using the gradient sending function; and the plaintext gradient is intercepted and encrypted by using the first aspect program to obtain a ciphertext gradient, and the ciphertext gradient is sent to the federated learning server, so that the federated learning server decrypts received ciphertext gradients sent by federated learning devices, and updates parameters of the to-be-trained model based on the plaintext gradients obtained after the decryption. According to the federated learning methods and apparatuses in this application, the plaintext gradient of the federated learning device is encrypted, and the encrypted ciphertext gradient is sent to the federated learning server, thereby reducing privacy leakage caused by acquisition of the plaintext gradient by an attacker.

FIG. 1