CLAIMS

What is claimed is:

1. A model training method, used to obtain a risk control model with a risk user identification capability through training by using a federated system, wherein the federated system comprises a control device and M participating devices located in different regions, M is an integer greater than 1, each participating device stores a local dataset, the local dataset comprises at least a user feature of a sample user in a region in which the participating device is located, wherein the M participating devices comprise at least a first participating device and a second participating device, the first participating device stores a first local dataset comprising a user feature and a risk label of a first sample user in a first region in which the first participating device is located, and the second participating device stores a second local dataset comprising a user feature of a second sample user in a second region in which the second participating device is located, wherein at least one training sample in the second local dataset does not comprise a corresponding risk label, and the method is applied to the control device, and comprises:

initializing a parameter of the risk control model; and

controlling the M participating devices to perform a plurality of times of iterative joint training on the risk control model until a preset training end condition is reached, to obtain a target parameter of the risk control model, wherein a process of each iteration comprises:

distributing a current model parameter of the risk control model to the M participating devices, so that the M participating devices each determine intermediate training information based on the current model parameter and the local dataset corresponding to each of the M participating devices, wherein the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset, wherein the first participating device performs supervised learning based on the current model parameter and the first local dataset to determine first intermediate training information, and the second participating device performs unsupervised learning based on the current model parameter and the second local dataset to determine second intermediate training information; and

obtaining the intermediate training information from each of the M participating devices, and updating the current model parameter of the risk control model based on M pieces of obtained

intermediate training information, wherein the M pieces of obtained intermediate training information comprise the first intermediate training information and the second intermediate training information, and wherein the trained risk control model is used to identify whether a user in the second region is a risk user.

2. The method according to claim 1, wherein the method further comprises:

sending first indication information to each of the M participating devices, wherein the first indication information is used to indicate N target feature dimensions, so that the M participating devices each generate the local dataset based on the N target feature dimensions, wherein N is an integer greater than or equal to 1.

3. The method according to claim 2, wherein the method further comprises:

receiving second indication information from each of the M participating devices, wherein the second indication information is used to indicate a plurality of candidate feature dimensions; and

determining the N target feature dimensions based on the M pieces of received second indication information.

4. The method according to claim 1, wherein the intermediate training information comprises gradient information, the gradient information represents a gradient of a loss function with respect to the current model parameter, and the loss function is used to determine a loss status of risk prediction performed by the participating device on the sample user based on the current model parameter; and

the updating the current model parameter of the risk control model based on M pieces of obtained intermediate training information comprises:

aggregating the gradient information in the M pieces of intermediate training information, to obtain aggregated gradient information; and

updating the current model parameter of the risk control model based on the aggregated gradient information.

5. The method according to claim 4, wherein the aggregating the gradient information in the M pieces of intermediate training information, to obtain aggregated gradient information comprises:

obtaining a quantity of sample users in the local dataset corresponding to each of the M participating devices;

determining a training weight corresponding to each of the M participating devices based on the quantity; and

aggregating M pieces of gradient information in the M pieces of intermediate training information based on the training weight, to obtain the aggregated gradient information.

6. The method according to claim 1, wherein the obtaining the intermediate training information from each of the M participating devices comprises:

obtaining a ciphertext from each of the M participating devices; and

decrypting the ciphertext by using a private key, to obtain the intermediate training information.

7. The method according to claim 1, wherein after the target parameter of the risk control model is obtained, the method further comprises:

sending the target parameter of the risk control model to each of the M participating devices.

8. A model training method, used to obtain a risk control model with a risk user identification capability through training by using a federated system, wherein the federated system comprises a control device and M participating devices located in different regions, M is an integer greater than 1, each participating device stores a local dataset, the local dataset comprises at least a user feature of a sample user in a region in which the participating device is located, wherein the M participating devices comprise at least a first participating device and a second participating device, the first participating device stores a first local dataset comprising a user feature and a risk label of a first sample user in a first region in which the first participating device is located, and the second participating device stores a second local dataset comprising a user feature of a second sample user in a second region in which the second participating device is located, wherein at least one training sample in the second local dataset does not comprise a corresponding risk label, and the method is applied to the participating device, the participating device being the first participating device or the second participating device, and comprises:

receiving a current model parameter of the risk control model from the control device;

determining intermediate training information based on the current model parameter and the local dataset corresponding to the participating device, wherein the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset, wherein, when the participating device is the first participating device, the determining comprises performing supervised learning based on the current model parameter and

the first local dataset to determine first intermediate training information, and, when the participating device is the second participating device, the determining comprises performing unsupervised learning based on the current model parameter and the second local dataset to determine second intermediate training information; and

sending the intermediate training information to the control device, so that the control device updates the current model parameter of the risk control model based on the intermediate training information corresponding to each of the M participating devices, wherein the intermediate training information corresponding to the M participating devices comprises the first intermediate training information and the second intermediate training information, and wherein the trained risk control model is used to identify whether a user in the second region is a risk user.

9. The method according to claim 8, wherein the method further comprises:

receiving first indication information from the control device, wherein the first indication information is used to indicate N target feature dimensions, and N is an integer greater than or equal to 1; and

generating the local dataset based on the N target feature dimensions.

10. The method according to claim 9, wherein the method further comprises:

sending second indication information to the control device, wherein the second indication information is used to indicate a plurality of candidate feature dimensions, so that the control device determines the N target feature dimensions based on the plurality of candidate feature dimensions.

11. The method according to claim 8, wherein the determining intermediate training information based on the current model parameter and the local dataset corresponding to the participating device comprises:

determining gradient information based on the current model parameter and the local dataset corresponding to the participating device, wherein the gradient information represents a gradient of a loss function related to the current model parameter, and the loss function is used to determine a loss status of risk prediction performed by the participating device on the sample user based on the current model parameter; and

the sending the intermediate training information to the control device comprises:

sending the gradient information to the control device, so that the control device obtains, based on the gradient information, aggregated gradient information used to update the current

model parameter.

12. The method according to claim 11, wherein the method further comprises:

sending a quantity of sample users in the local dataset to the control device, so that the control device obtains the aggregated gradient information based on the quantity and the gradient information.

13. The method according to claim 8, wherein the sending the intermediate training information to the control device comprises:

encrypting the intermediate training information by using a public key, to generate a ciphertext; and

sending the ciphertext to the control device.

14. The method according to claim 8, wherein the method further comprises:

receiving a target parameter of the risk control model from the control device, wherein the target parameter is a model parameter of the trained risk control model.

15. An electronic device, located in a federated system that comprises a control device and M participating devices, wherein the federated system is configured to obtain a risk control model with a risk user identification capability through training, the M participating devices are located in different regions, each participating device stores a local dataset, the local dataset comprises at least a user feature of a sample user in a region in which the participating device is located, wherein the M participating devices comprise at least a first participating device and a second participating device, the first participating device stores a first local dataset comprising a user feature and a risk label of a first sample user in a first region in which the first participating device is located, and the second participating device stores a second local dataset comprising a user feature of a second sample user in a second region in which the second participating device is located, wherein at least one training sample in the second local dataset does not comprise a corresponding risk label, and the electronic device serves as the control device, and comprises:

at least one storage medium, storing at least one instruction set; and

at least one processor, communicatively connected to the at least one storage medium, wherein when running, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set:

initializing a parameter of the risk control model; and

controlling the M participating devices to perform a plurality of times of iterative joint

training on the risk control model until a preset training end condition is reached, to obtain a target parameter of the risk control model, wherein a process of each iteration comprises:

distributing a current model parameter of the risk control model to the M participating devices, so that the M participating devices each determine intermediate training information based on the current model parameter and the local dataset corresponding to each of the M participating devices, wherein the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset, wherein the first participating device performs supervised learning based on the current model parameter and the first local dataset to determine first intermediate training information, and the second participating device performs unsupervised learning based on the current model parameter and the second local dataset to determine second intermediate training information; and

obtaining the intermediate training information from each of the M participating devices, and updating the current model parameter of the risk control model based on M pieces of obtained intermediate training information, wherein the M pieces of obtained intermediate training information comprise the first intermediate training information and the second intermediate training information, and wherein the trained risk control model is used to identify whether a user in the second region is a risk user.

16. The electronic device according to claim 15, wherein the at least one processor further performs the following operations:

sending first indication information to each of the M participating devices, wherein the first indication information is used to indicate N target feature dimensions, so that the M participating devices each generate the local dataset based on the N target feature dimensions, wherein N is an integer greater than or equal to 1.

17. An electronic device, located in a federated system that comprises a control device and M participating devices, wherein the federated system is configured to obtain a risk control model with a risk user identification capability through training, the M participating devices are located in different regions, each participating device stores a local dataset, the local dataset comprises at least a user feature of a sample user in a region in which the participating device is located, wherein the M participating devices comprise at least a first participating device and a second participating device, the first participating device stores a first local dataset comprising a user feature and a risk label of a first sample user in a first region in which the first participating device is located, and

the second participating device stores a second local dataset comprising a user feature of a second sample user in a second region in which the second participating device is located, wherein at least one training sample in the second local dataset does not comprise a corresponding risk label, and the electronic device serves as the first participating device or the second participating device, and comprises:

at least one storage medium, storing at least one instruction set; and

at least one processor, communicatively connected to the at least one storage medium, wherein when running, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set:

receiving a current model parameter of the risk control model from the control device;

determining intermediate training information based on the current model parameter and the local dataset corresponding to the participating device, wherein the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset, wherein, when the electronic device serves as the first participating device, the determining comprises performing supervised learning based on the current model parameter and the first local dataset to determine first intermediate training information, and, when the electronic device serves as the second participating device, the determining comprises performing unsupervised learning based on the current model parameter and the second local dataset to determine second intermediate training information; and

sending the intermediate training information to the control device, so that the control device updates the current model parameter of the risk control model based on the intermediate training information corresponding to each of the M participating devices, wherein the intermediate training information corresponding to the M participating devices comprises the first intermediate training information and the second intermediate training information, and wherein the trained risk control model is used to identify whether a user in the second region is a risk user.

18. A computer-readable non-transitory storage medium, wherein the computer-readable non-transitory storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the method according to any one of claims 1 to 7 is implemented, or the method according to any one of claims 8 to 14 is implemented.