

MODEL TRAINING METHOD, DEVICE, AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to a model training method, a device, and a storage medium.

5

BACKGROUND

[0002] With rapid development of Internet technologies, more people enjoy convenience services on various service platforms. In this case, some unauthorized persons speculate on the service platform, to pose a risk to the service platform or a normal user. In this case, the service platform needs to train a risk control model used to identify a risk user, to ensure security of the service platform or the normal user. Therefore, how to obtain a risk control model with a relatively good risk control effect on the service platform is a problem that needs to be resolved urgently.

10

[0003] Content of the background part is merely information learned of by the inventor, and neither means that the information has entered a public domain before an application date of this disclosure, nor means that the information can become a conventional technology of this disclosure.

15

SUMMARY

[0004] This specification provides a model training method, a device, and a storage medium. A plurality of participants perform joint training, to obtain a risk control model. In a training process, local data of the plurality of participants is fully used, to break a data island, and improve a risk control effect of the risk control model.

20

[0005] According to a first aspect, this specification provides a model training method, used to obtain a risk control model with a risk user identification capability through training by using a federated system, where the federated system includes 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 includes at least a user feature of a sample user in a region in which the participating device is located, and the method is applied to the control device. The method

25

includes: 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, where a process of each iteration includes: 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, where the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset; 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.

[0006] According to a second aspect, this specification provides a model training method, used to obtain a risk control model with a risk user identification capability through training by using a federated system, where the federated system includes 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 includes at least a user feature of a sample user in a region in which the participating device is located, and the method is applied to the participating device. The method includes: 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, where the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset; 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.

[0007] According to a third aspect, this specification further provides an electronic device, located in a federated system that includes a control device and M participating devices, where 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 includes at least a user feature of a sample user in a region in which the participating device is located, and the electronic device serves as the control device, and includes: 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, where 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, where a process of each iteration includes: 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, where the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset; 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.

[0008] According to a fourth aspect, this specification further provides an electronic device, located in a federated system that includes a control device and M participating devices, where 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 includes at least a user feature of a sample user in a region in which the participating device is located, and the electronic device serves as one of the M participating devices, and includes: 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, where 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, where the intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset; 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.

[0009] According to a fifth aspect, this specification provides a risk user identification method, including: obtaining a user feature of a target user; inputting the user feature of the target user into a trained risk control model, to obtain a risk probability output by the risk control model; and determining, based on the risk probability, whether the target user is a risk user, where the risk control model is obtained through training by using a federated system, the federated system includes a control device and M participating devices, M is an integer greater than 1, and in the training process, the control device performs the method according to the first aspect and the participating device performs the method according to the second aspect.

[0010] According to a sixth aspect, this specification provides an electronic device, including at least one storage medium and at least one processor. The at least one storage medium stores at least one instruction set. The at least one processor is communicatively connected to the at least one instruction set. 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: obtaining a user feature of a target user; inputting the user feature of the target user into a trained risk control model, to obtain a risk probability output by the risk control model; and determining, based on the risk probability, whether the target user is a risk user, where the risk control model is obtained through training by using a federated system, the federated system includes a control device and M participating devices, M is an integer greater than 1, and in the training process, the control device performs the method according to the first aspect and the participating device performs the method according to the second aspect.

[0011] According to a seventh aspect, this specification provides a computer-readable non-transitory storage medium. 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 training method according to the first aspect or the second aspect is implemented, or the identification method according to the fifth aspect is implemented.

[0012] Other functions of the model training method, the device, and the storage medium provided in this specification are partially listed in the following descriptions. Based on the descriptions, content described by using the following numbers and examples is clear to a person of ordinary skill in the art. The creative aspects of the model training method, the device, and the storage medium provided in this specification can be fully explained by practice or by using the method, apparatus, and combination described in the following detailed example.

BRIEF DESCRIPTION OF DRAWINGS

[0013] To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following description show merely some
5 embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0014] FIG. 1 is a schematic diagram of an application scenario of model training according to an embodiment of this specification;

[0015] FIG. 2 is a diagram of a hardware structure of an electronic device according to an
10 embodiment of this specification;

[0016] FIG. 3 is a flowchart of a model training method according to an embodiment of this specification; and

[0017] FIG. 4 is a detailed flowchart of a model training method according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0018] Specific application scenarios and requirements of this specification are provided in the following descriptions, so that a person skilled in the art can manufacture and use content of this specification. For the person skilled in the art, various local modifications to the disclosed
20 embodiments are apparent, and the general principles defined herein can be applied to other embodiments and applications without departing from the spirit and scope of this specification. Therefore, this specification is not limited to the shown embodiments, but has a widest scope consistent with that of the claims.

[0019] The terms used herein are only intended to describe a particular example embodiment, but do not impose a limitation. For example, unless otherwise specified in the context, the singular
25 forms "one", "a", and "the" used herein can also include a plural form. When used in this specification, the terms "include", "comprise", and/or "have" indicate/indicates existence of an associated integer, step, operation, element, and/or component, but does not exclude existence of one or more other features, integers, steps, operations, elements, components, and/or groups, or another feature, integer, step, operation, element, component, and/or group can be added to the

system/method.

[0020] In consideration of the following descriptions, these and other features of this specification, operations and functions of related components of the structure, and economy of combination and manufacturing of components can be significantly improved. With reference to the accompanying drawings, all of these form a part of this specification. However, it should be clearly understood that the accompanying drawings are merely used for the purpose of illustration and description, and are not intended to limit the scope of this specification. It should be further understood that the accompanying drawings are not drawn to scale.

[0021] The flowchart used in this specification illustrates operations implemented by a system in some embodiments of this specification. It should be clearly understood that operations in the flowchart can be implemented out of sequence. On the contrary, operations can be implemented reversely or simultaneously. In addition, one or more other operations can be added to the flowchart. One or more operations can be removed from the flowchart.

[0022] A service platform can obtain a risk control model through training based on data on the platform. For example, the service platform needs to train a risk control model used to identify a risk user in a marketing scenario. In this case, the service platform can obtain user features of a plurality of sample users through cleaning from the data on the platform, to form a training sample, and obtain the risk control model through training based on the training sample.

[0023] However, for a newly developed service platform, there is a relatively small amount of data on the platform and limited risk control experience, and it is difficult to obtain the risk control model through training based on the data on the platform.

[0024] For example, in an initial stage of development, the service platform launches many marketing activities to attract users. In this case, an unauthorized person is also attracted to extract marketing funds of the service platform by using a cheating behavior, or many users who take advantage of loopholes use the service platform only during an activity. Therefore, the service platform needs to identify a risk user in the marketing scenario by using an effective risk control model, to reduce a marketing asset loss of the platform, and avoid a problem that an expected marketing effect cannot be achieved because the marketing funds of the platform are illegally extracted by the unauthorized person.

[0025] In this case, the service platform can refer to risk control models of some other service platforms that are developed earlier and that have a large amount of historical data, to avoid some

risks. However, because different service platforms face different user groups and develop different service types, different service platforms prevent and control different risks. It is difficult to accurately and comprehensively prevent and control a risk of the service platform by referring to the risk control models of the other service platforms.

5 **[0026]** In addition, the service platform can entrust another service platform with rich risk control experience to train the risk control model for the service platform. In this case, the data on the service platform needs to be further combined in a training process. However, due to a data privacy problem, data cannot be shared between different service platforms. In particular, for example, when the another service platform and the service platform belong to different countries
10 or regions, because of a limitation of transferring user data abroad, the another service platform cannot obtain real data of the service platform, and therefore, cannot train the risk control model for the service platform in a software as a service (SaaS) manner.

[0027] In view of this, this specification provides a model training method, a device, and a storage medium. A federated system that includes a control device and a plurality of participating
15 devices performs a plurality of times of iterative joint training, to obtain a risk control model that can identify a risk user. In a process of each time of iterative training, the control device performs coordination, to complete training of the risk control model while a local dataset of the participating device is only used locally, thereby facilitating data privacy protection. In addition, in the training process, local datasets from the plurality of participating devices are used to break
20 a data island, so that training data is more diversified, to improve a generalization capability and adaptability of the risk control model obtained through training, and improve a risk control effect of the risk control model.

[0028] The following describes, with reference to FIG. 1, an application scenario of risk control model training provided in this specification.

25 **[0029]** FIG. 1 is a schematic diagram of an application scenario of model training according to an embodiment of this specification. As shown in FIG. 1, a scenario 001 shows an example of a federated system that trains a risk control model, and the federated system includes a control device 100 and a plurality of participating devices 200.

[0030] As a controller of joint training, the control device 100 can coordinate and control each
30 participating device 200 to participate in a plurality of times of iterative training, until performance of the risk control model satisfies a preset condition. The control device 100 and the participating

device 200 can establish a communication connection, to transmit data to each other. For example, in each time of iterative training, the control device 100 can distribute a current model parameter of the risk control model to each participating device 200, so that the participating device 200 trains the risk control model based on the current model parameter, to obtain intermediate training information. The control device 100 can further obtain the intermediate training information from each of the plurality of participating devices 200. The control device 100 can update the current model parameter of the risk control model based on the intermediate training information. After the plurality of times of iterative training, the control device 100 obtains a risk control model that satisfies the preset condition.

10 **[0031]** The control device 100 is a device with a certain data processing capability. The control device 100 can execute data and instructions of a model training method described in this specification, and can execute or be configured to execute the data and instructions. In some embodiments, the control device 100 can include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

15 **[0032]** Different participating devices 200 can be located in different regions (for example, countries or regions), each participating device 200 stores a local dataset, and the different participating devices 200 can be service devices of the same type of service platform in different regions. One participating device 200 is used as an example. A local dataset of the participating device 200 includes a user feature of a user in a region in which the participating device 200 is located. For example, the participating device 200 is a service device of a service platform in a country A, and platform data that can be obtained includes but is not limited to personal basic information (for example, a user name, a city, or contact information) that is registered by a user in the country A on the service platform, event information (for example, an rights and interests granting event, a payment event, etc. in a marketing scenario) of an event that is executed by the user in the country A on the service platform, etc. The participating device 200 can obtain, through cleaning based on the platform data, a user feature used to train the risk control model. The user feature is, for example, a consumption frequency, a payment success rate, and a quantity of times of participating in a marketing activity. Further, the participating device 200 can generate the local dataset based on the user feature. Subsequently, in each time of iterative training, the participating device 200 can train the risk control model based on the local dataset and the current model parameter sent by the control device 100, to obtain the intermediate training information, and send

20

25

30

the intermediate training information and other information required by the control device 100 (for example, a quantity of sample users) to the control device 100.

[0033] After the risk control model is trained, the control device 100 can send a target parameter of the risk control model to the participating device 200, and the participating device 5 200 can install the risk control model on a risk control execution device (not shown in FIG. 1). For example, the participating device 200 can install the risk control model on a marketing server in a region in which the participating device 200 is located, to identify a risk user in a marketing scenario. Identifying the risk user in the marketing scenario can be understood as identifying whether a user participating in the marketing activity is a risk user. The marketing activity is, for 10 example, that the service platform grants rights and interests to a user of the service platform. In this specification, the rights and interests are rights and interests of the user on the service platform. For example, the user has the right to enjoy price reduction when purchasing a product or a service on the service platform, and the user has the right to obtain the rights and interests when a certain condition is satisfied (for example, in a case of a new user on the service platform). The rights and 15 interests can include but are not limited to a cash, a discount coupon, a full coupon, a single item coupon, a coupon, a gift, an integral, etc. Specifically, when the risk control model identifies that a user who currently participates in the marketing activity is a risk user, the service platform can refuse to send the rights and interests to the user; or when the risk control model identifies that a user who currently participates in the marketing activity is not a risk user, the service platform can 20 normally send the rights and interests to the user; or when the risk control model cannot determine whether a user who currently participates in the marketing activity is a risk user, the service platform can further determine, based on another risk control policy, whether the user is a risk user.

[0034] The participating device 200 is a device with a certain data processing capability. The participating device 200 can execute data and instructions of a model training method described 25 in this specification, and can execute or be configured to execute the data and instructions. In some embodiments, the participating device 200 can include a hardware device with a data information processing function and a necessary program needed for driving the hardware device to work.

[0035] It should be understood that a quantity of participating devices 200 in FIG. 1 is merely an example. Based on an implementation requirement, there can be any quantity of participating 30 devices 200.

[0036] It should be noted that, the model training method is partially performed on the control

device 100, and is partially performed on the participating device 200.

[0037] FIG. 2 is a diagram of a hardware structure of an electronic device 300 according to an embodiment of this specification. The electronic device 300 can serve as the control device 100 in FIG. 1, or can serve as any participating device 200 in FIG. 1.

5 **[0038]** As shown in FIG. 2, the electronic device 300 can include at least one storage medium 330 and at least one processor 320. In some embodiments, the electronic device 300 can further include a communication port 350 and an internal communication bus 310. In addition, the electronic device 300 can further include an I/O component 360.

[0039] The internal communication bus 310 can be connected to different system components.
10 For example, the internal communication bus 310 can be connected to the storage medium 330, the processor 320, the communication port 350, and the I/O component 360.

[0040] The I/O component 360 supports an input/output between the electronic device 300 and another component.

[0041] The communication port 350 is used for data communication between the electronic
15 device 300 and the outside. For example, the communication port 350 can be used for data communication between the electronic device 300 and a network 400. The communication port 350 can be a wired communication port, or can be a wireless communication port.

[0042] The network 400 is a medium configured to provide a communication connection
between the control device 100 and the participating device 200. The network 400 can facilitate
20 exchange of information or data. In some embodiments, the network 400 can be any type of wired or wireless network, or a combination thereof. For example, the network 400 can include a cable network, a wired network, an optical fiber network, a telecommunications network, an intranet, the Internet, a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), a metropolitan area network (MAN), a public switched telephone network
25 (PSTN), a Bluetooth network, a ZigBee network, a near field communication (NFC) network, or a similar network. In some embodiments, the network 400 can include one or more network access points. For example, the network 400 can include a wired or wireless network access point, for example, a base station or an Internet switching point. Through the access point, one or more components in the control device 100 and the participating device 200 can be connected to the
30 network 400 to exchange data or information.

[0043] The storage medium 330 can include a data storage apparatus. The data storage

apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 332, a read-only storage medium (ROM) 334, or a random access storage medium (RAM) 336. The storage medium 330 further includes at least one instruction set stored in the data storage apparatus. The instruction set
5 can include computer program code. The computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, etc. for performing the model training method provided in this specification.

[0044] The processor 320 can be communicatively connected to the storage medium 330. The processor 320 is configured to execute the at least one instruction set. When the electronic device
10 300 runs as the control device 100 or the participating device 200, the processor 320 reads the at least one instruction set, and performs, based on an indication of the at least one instruction set, the model training method provided in this specification.

[0045] The processor 320 can be in a form of one or more processors. In some embodiments, the processor 320 can include one or more hardware processors, for example, a microcontroller, a
15 microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit, processor, etc. that can perform
20 one or more functions, or any combination thereof.

[0046] To merely describe a problem, only one processor 320 is shown in the electronic device 300 in the accompanying drawings. However, it should be noted that the electronic device 300 in this specification can further include a plurality of processors. Therefore, the operations and/or method steps disclosed in this specification can be performed by one processor or can be jointly
25 performed by a plurality of processors. For example, if the processor 320 in the electronic device 300 in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or separately performed by two different processors 320 (for example, a first processor performs step A, and a second processor performs step B, or a first processor and a second processor jointly perform step A and step B).

[0047] FIG. 3 is a flowchart of a model training method P100 according to an embodiment of this specification. As described above, a control device 100 and a participating device 200 can
30

perform the method P100 in this specification through coordination. Specifically, a processor in the control device 100 can read an instruction set stored in a local storage medium of the control device 100, and then perform, based on a stipulation of the instruction set, steps or operations performed by the control device 100 in the method P100 in this specification. A processor in the participating device 200 can read an instruction set stored in a local storage medium of the participating device 200, and then perform, based on a stipulation of the instruction set, steps or operations performed by the participating device 200 in the method P100 of this specification.

[0048] The method P100 can be applied to various service platforms such as a payment platform, a transaction platform, a network security platform, and a financial platform that need to perform risk control. To clearly and completely describe the method P100, the following uses the payment platform as an example for description. An application of the method P100 to another service platform can be obtained by analogy.

[0049] For ease of description, the following provides descriptions by using an example in which a federated system includes a control device and M participating devices, where M is an integer greater than 1. Each participating device stores a local dataset, and the local dataset of the participating device includes at least a user feature of a sample user in a region in which the participating device is located. As shown in FIG. 3, the model training method P100 can include the following steps.

[0050] S110: The control device initializes a parameter of a risk control model.

[0051] The control device can obtain the initialized parameter of the risk control model through random initialization, Xavier (Glorot) initialization, He initialization, orthogonal initialization, etc.

[0052] After initialization is completed, the control device can control the M participating devices to perform a plurality of times of iterative joint training on the risk control model, and until the risk control model reaches a preset training end condition, the control device obtains a target parameter of the risk control model.

[0053] For example, in the M participating devices, some participating devices are service devices corresponding to a service platform with relatively much risk control experience, and some other participating devices are service devices corresponding to a service platform (for example, a newly developed service platform) with relatively little risk control experience.

[0054] In a process of each iteration, the control device distributes a current model parameter

of the risk control model to the M participating devices, and 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. The intermediate training information represents a risk prediction status of the risk control model for the sample user in the local dataset.

5 The control device can separately obtain, from the M participating devices, the intermediate training information determined by each participating device, and update the current model parameter of the risk control model based on the M pieces of obtained intermediate training information.

[0055] As shown in FIG. 3, in a process of the first iteration:

10 **[0056]** S120: The control device distributes a current model parameter #1 of the risk control model to the M participating devices, where the current model parameter #1 is the initialized parameter that is of the risk control model and that is obtained in S110.

[0057] For example, as shown in FIG. 4, it is assumed that the M participating devices include a first participating device and a second participating device. S120 includes S1201 and S1202. It
15 can be understood that, S1201 and S1202 can be performed simultaneously, or can be performed sequentially. This is not limited in this specification.

[0058] S1201: The control device sends the current model parameter #1 to the first participating device, and correspondingly, the first participating device receives the current model parameter #1.

20 **[0059]** S1202: The control device sends the current model parameter #1 to the second participating device, and correspondingly, the second participating device receives the current model parameter #1.

[0060] S130: Each of the M participating devices determines intermediate training information #1 based on the current model parameter #1 and the local dataset.

25 **[0061]** It can be understood that, before performing S130, each participating device needs to generate the local dataset of the participating device. The local dataset can be stored in a storage device in the region in which the participating device is located, or the local dataset can be stored in the participating device.

[0062] In some embodiments, the control device sends first indication information to each of
30 the M participating devices. The first indication information is used to indicate N target feature dimensions. The M participating devices each can generate the local dataset based on the N target

feature dimensions, where N is an integer greater than or equal to 1.

[0063] For example, for a marketing scenario, the N target feature dimensions include but are not limited to basic information of a user, a transaction frequency of the user, a transaction quantity, a transaction time interval, a payment success rate, a recharge quantity, a quantity of times that the user historically participates in a marketing activity, a frequency at which the user historically participates in the marketing activity, a marketing activity type that the user historically participates in, etc.

[0064] It can be understood that, the control device can obtain, through selection from feature dimensions used for risk control in a plurality of scenarios, the N target feature dimensions that are applicable to a specific scenario (for example, the marketing scenario). In addition, the control device can further obtain the N target feature dimensions in another manner.

[0065] In some embodiments, the control device receives second indication information from each of the M participating devices, where the second indication information is used to indicate a plurality of candidate feature dimensions; and determines the N target feature dimensions based on the M pieces of received second indication information.

[0066] For example, the M participating devices include a first participating device and a second participating device. Specifically, the first participating device can obtain first platform data on a first service platform, and determine $N1$ candidate feature dimensions from the first platform data; and the second participating device can obtain second platform data on a second service platform, and determine $N2$ candidate feature dimensions from the second platform data. The first participating device indicates the $N1$ candidate feature dimensions to the control device by using second indication information #1, and the second participating device indicates the $N2$ candidate feature dimensions to the control device by using second indication information #2. The control device determines the same candidate feature dimension in the $N1$ candidate feature dimensions and the $N2$ candidate feature dimensions, and uses the same candidate feature dimension as the N target feature dimensions.

[0067] In some embodiments, for data privacy, the second indication information #1 sent by the first participating device to the control device is a candidate feature dimension ciphertext #1. In other words, after determining the $N1$ candidate feature dimensions, the first participating device encrypts the $N1$ candidate feature dimensions by using a public key, to obtain the candidate feature dimension ciphertext #1. After receiving the candidate feature dimension ciphertext #1, the

control device can decrypt the candidate feature dimension ciphertext #1 by using a private key corresponding to the public key, to obtain the N1 candidate feature dimensions.

[0068] Similarly, the second indication information #2 sent by the second participating device to the control device is a candidate feature dimension ciphertext #2. In other words, after determining the N2 candidate feature dimensions, the second participating device encrypts the N2 candidate feature dimensions by using the public key, to obtain the candidate feature dimension ciphertext #2. After receiving the candidate feature dimension ciphertext #2, the control device can decrypt the candidate feature dimension ciphertext #2 by using the private key, to obtain the N2 candidate feature dimensions.

[0069] It can be understood that before joint training, the control device can generate the public key and the private key, locally store the private key in the control device, and send the public key to each participating device. Each participating device locally stores the public key. Each participating device and the control device transfer a candidate feature dimension in a ciphertext form, to improve security in an information transfer process.

[0070] After determining the N target feature dimensions, the control device indicates the N target feature dimensions to the first participating device and the second participating device by using the first indication information. The first participating device generates a first local dataset based on the N target feature dimensions, and locally stores the first local dataset in the first participating device for training. The first local dataset includes a user feature of a first sample user in a region in which the first participating device is located and a risk label of the first sample user. The second participating device generates a second local dataset based on the N target feature dimensions, and locally stores the second local dataset in the second participating device for training. The second local dataset includes a user feature of a second sample user in a region in which the second participating device is located.

[0071] Specifically, the first participating device uses, as the first sample user, a user who uses the first service platform, and obtains the user feature and the risk label of the first sample user from the first platform data based on the N target feature dimensions. The user feature includes a user feature corresponding to the N target feature dimensions in the above-mentioned example, and the risk label includes a normal user or a risk user. In addition, all user features and risk labels corresponding to one first sample user are used as one training sample in the first local dataset, and the first participating device generates, in this manner, the first local dataset that includes a

plurality of training samples.

[0072] The second participating device uses, as the second sample user, a user who uses the second service platform, and obtains the user feature of the second sample user from the second platform data based on the N target feature dimensions. The user feature includes a user feature corresponding to the N target feature dimensions in the above-mentioned example. In addition, all user features corresponding to one second sample user are used as one training sample in the second local dataset, and the second participating device generates, in this manner, the second local dataset that includes a plurality of training samples.

[0073] It can be understood that the first platform data and the second platform data can be data in the same time period, for example, platform data in the same year. Therefore, a case in which there is a small quantity of same candidate feature dimensions in candidate feature dimensions of both parties because platform data belongs to different time periods can be avoided, and consequently, an effect of the risk control model obtained through training is poor.

[0074] After each participating device generates the local dataset, the intermediate training information #1 can be determined based on the current model parameter #1 and the local dataset. The current model parameter #1 can be understood as the current model parameter of the risk control model in the process of the first iteration. The intermediate training information #1 can be understood as the intermediate training information obtained by the participating device in the process of the first iteration. The intermediate training information #1 obtained by each participating device in the process of the first iteration is different.

[0075] For example, as shown in FIG. 4, S130 includes S1301 and S1302.

[0076] S1301: The first participating device determines intermediate training information #1a based on the current model parameter #1 and a local dataset #1a.

[0077] After generating the first local dataset, the first participating device can divide the first local dataset into n local datasets, where n is an integer greater than 1. For example, the first local dataset includes the local dataset #1a, a local dataset #2a, ..., and a local dataset #na. Each local dataset participates in one time of iterative training, and all local datasets can include the same quantity of sample users or different quantities of sample users.

[0078] In some embodiments, intermediate training information determined by each participating device in each iteration can include gradient information. For example, the intermediate training information #1a includes gradient information #1a, the first participating

device determines the gradient information #1a based on the current model parameter #1 and the local dataset #1a, the gradient information #1a represents a gradient of a loss function 1 with respect to the current model parameter #1, and the loss function 1 is used to determine a loss status of risk prediction performed by the first participating device on a sample user in the local dataset #1a based on the current model parameter #1. The gradient information #1a can be calculated according to the following formula.

$$\nabla L_1(\theta, D_1) = \frac{1}{|D_1|} \sum_{x_1 \in D_1} \nabla l_1(\theta, x_1)$$

[0079] Herein, L_1 is the loss function 1, $\nabla L_1(\theta, D_1)$ is the gradient information #1a, D_1 is a quantity of sample users in the local dataset #1a, and $\nabla l_1(\theta, x_1)$ is a gradient of a loss l_1 of a single sample x_1 in the local dataset #1a with respect to a parameter θ (namely, the current model parameter #1).

[0080] In some embodiments, the intermediate training information determined by each participating device in each iteration can include a model parameter updating manner. For example, the intermediate training information #1a includes a difference between an updated parameter and the current model parameter θ . If the updated parameter is denoted as θ_1 , the intermediate training information #1a can include $\Delta\theta_1$:

$$\Delta\theta_1 = \theta_1 - \theta = -\eta_1 \cdot \nabla L_1$$

[0081] Herein, η_1 denotes a learning rate at which the first participating device trains the risk control model.

[0082] In some embodiments, the intermediate training information determined by each participating device in each iteration can include a loss function. For example, the intermediate training information #1a can include the sum of losses of all samples in the local dataset #1a.

[0083] S1302: The second participating device determines intermediate training information #1b based on the current model parameter #1 and a local dataset #1b.

[0084] After generating the second local dataset, the second participating device can divide the second local dataset into n local datasets. For example, the second local dataset includes the local dataset #1b, a local dataset #2b, ..., and a local dataset #nb. Each local dataset participates in one time of iterative training, and all local datasets can include the same quantity of sample users or different quantities of sample users.

[0085] In some embodiments, intermediate training information determined by each participating device in each iteration can include gradient information. For example, the intermediate training information #1b includes gradient information #1b, the second participating device determines the gradient information #1b based on the current model parameter #1 and the local dataset #1b, the gradient information #1b represents a gradient of a loss function 2 with respect to the current model parameter #1, and the loss function 2 is used to determine a loss status of risk prediction performed by the second participating device on a sample user in the local dataset #1b based on the current model parameter #1. The gradient information #1b can be calculated according to the following formula.

$$\nabla L_2(\theta, D_2) = \frac{1}{|D_2|} \sum_{x_2 \in D_2} \nabla l_2(\theta, x_2)$$

[0086] Herein, L_2 is the loss function 2, $\nabla L_2(\theta, D_2)$ is the gradient information #1b, D_2 is a quantity of sample users in the local dataset #1b, and $\nabla l_2(\theta, x_2)$ is a gradient of a loss l_2 of a single sample x_2 in the local dataset #1b with respect to a parameter θ (namely, the current model parameter #1).

[0087] In some embodiments, the intermediate training information determined by each participating device in each iteration can include a model parameter updating manner. For example, the intermediate training information #1b includes a difference between an updated parameter and the current model parameter θ . If the updated parameter is denoted as θ_2 , the intermediate training information #1b can include $\Delta\theta_2$:

$$\Delta\theta_2 = \theta_2 - \theta = -\eta_2 \cdot \nabla L_2$$

[0088] Herein, η_2 denotes a learning rate at which the second participating device trains the risk control model.

[0089] In some embodiments, the intermediate training information determined by each participating device in each iteration can include a loss function. For example, the intermediate training information #1b can include the sum of losses of all samples in the local dataset #1b.

[0090] It can be understood that because a training sample in the first local dataset generated by the first participating device includes a risk label, the first participating device performs supervised learning in a model training process; and because some training samples in the second local dataset generated by the second participating device do not include a risk label, the second

participating device performs unsupervised learning in a model training process. It can be learned that the first participating device and the second participating device use different loss functions in the model training processes. A loss function of supervised learning is, for example, a cross-entropy loss function or a mean squared error loss function; and a loss function of unsupervised learning is, for example, a reconstruction error function or a distance measurement function.

[0091] S140: The M participating devices each send, to the control device, the intermediate training information #1 obtained by each of the M participating devices.

[0092] For example, as shown in FIG. 4, S140 includes S1401 and S1402.

[0093] S1401: The first participating device sends the intermediate training information #1a to the control device, and correspondingly, the control device receives the intermediate training information #1a.

[0094] For example, the intermediate training information #1a is an intermediate training information ciphertext #1a. After determining the intermediate training information #1a, the first participating device encrypts the intermediate training information #1a by using the public key, to obtain the intermediate training information ciphertext #1a, and sends the intermediate training information ciphertext #1a to the control device. The control device can decrypt the intermediate training information ciphertext #1a by using the private key, to obtain the intermediate training information #1a.

[0095] S1402: The second participating device sends the intermediate training information #1b to the control device, and correspondingly, the control device receives the intermediate training information #1b.

[0096] For example, the intermediate training information #1b is an intermediate training information ciphertext #1b. After determining the intermediate training information #1b, the second participating device encrypts the intermediate training information #1b by using the public key, to obtain the intermediate training information ciphertext #1b, and sends the intermediate training information ciphertext #1b to the control device. The control device can decrypt the intermediate training information ciphertext #1b by using the private key, to obtain the intermediate training information #1b.

[0097] Each participating device and the control device transfer intermediate training information in a ciphertext form, to improve security in an information transfer process, and avoid information disclosure.

[0098] S150: The control device updates the current model parameter #1 of the risk control model based on the M pieces of intermediate training information #1, to obtain a current model parameter #2.

[0099] For example, if the intermediate training information #1a obtained by the control device includes gradient information #1a, and the intermediate training information #1b obtained by the control device includes gradient information #1b, the control device can obtain a quantity D_1 of sample users in the local dataset #1a from the first participating device, and obtain a quantity D_2 of sample users in the local dataset #1b from the second participating device. The control device can determine a training weight #1 corresponding to the first participating device and a training weight #2 corresponding to the second participating device based on D_1 and D_2 . For example, the training weight #1 is $\frac{|D_1|}{|D_1|+|D_2|}$, and the training weight #2 is $\frac{|D_2|}{|D_1|+|D_2|}$. After obtaining the gradient information #1a, the gradient information #1b, the training weight #1, and the training weight #2, the control device can obtain aggregated gradient information ΔL according to the following formula.

$$\Delta L = \frac{1}{|D_1|+|D_2|} (|D_1| \cdot \nabla L_1 + |D_2| \cdot \nabla L_2)$$

[0100] Further, the control device can determine the current model parameter #2 based on the aggregated gradient information. For example, the current model parameter #2 is obtained according to the following formula:

$$\theta' = \theta - \eta \cdot \Delta L$$

[0101] Herein, θ' denotes an updated current model parameter #2, η denotes a learning rate at which the control device trains the risk control model, ΔL denotes an aggregation gradient, and η , η_1 , and η_2 can be the same or different.

[0102] For example, if the intermediate training information #1a obtained by the control device includes $\Delta\theta_1$, and the intermediate training information #1b obtained by the control device includes $\Delta\theta_2$, the control device can obtain η_1 and η_2 from the first participating device and the second participating device, determine the gradient information #1a based on $\Delta\theta_1$ and η_2 , and determine the gradient information #1b based on $\Delta\theta_2$ and η_2 . Subsequently, the control device can determine the current model parameter #2 in a manner in the above-mentioned example.

[0103] For example, if the intermediate training information #1a obtained by the control device includes the sum #1a of losses of all samples in the local dataset #1a, the control device can determine the gradient information #1a based on the sum #1a of the losses and D_1 ; and if the intermediate training information #1b obtained by the control device includes the sum #1b of losses of all samples in the local dataset #1b, the control device can determine the gradient information #1b based on the sum #1b of the losses and D_2 . Subsequently, the control device can determine the current model parameter #2 in a manner in the above-mentioned example.

[0104] So far, the first time of iterative training ends. By analogy, after $n-1$ times of iterative training, the control device can determine, based on the preset training end condition, whether the risk control model corresponding to the current model parameter #n needs to continue to be trained; and if it is determined that training does not need to be continued, the current model parameter #n is used as the target parameter of the risk control model; or if it is determined that training needs to be continued, the n^{th} time of iterative training is performed. The current model parameter #n is a current model parameter that is of the risk control model and that is obtained through updating by the control device through the $(n-1)^{\text{th}}$ time of iterative training.

[0105] The training end condition can include a preset quantity of iterations. In other words, after a quantity of iterations reaches the preset quantity of iterations, model training can be stopped. Alternatively, the training end condition can include that both the loss function 1 and the loss function 2 converge. Alternatively, the training end condition can include a condition related to performance of a verification set. For example, in a process of the $(n-1)^{\text{th}}$ time of iterative training, the first participating device can determine a first accuracy rate corresponding to a current model parameter #n-1 based on a verification set generated based on the first platform data, and send the first accuracy rate to the control device; and in the process of the $(n-1)^{\text{th}}$ time of iterative training, the second participating device can determine a second accuracy rate corresponding to the current model parameter #n-1 based on a verification set generated based on the second platform data, and send the second accuracy rate to the control device. When determining that both the first accuracy rate and the second accuracy rate reach a preset accuracy rate, the control device can determine that training ends. If one of the first accuracy rate or the second accuracy rate does not reach the preset accuracy rate, the control device determines that the n^{th} time of iterative training further needs to be performed. Alternatively, the training end condition can be another condition. Conditions are not listed one by one.

[0106] In a process of the n^{th} iteration:

[0107] S12x: The control device distributes the current model parameter #n of the risk control model to the M participating devices, where the current model parameter #n is a model parameter updated by the control device in a process of the $(n-1)^{\text{th}}$ iteration.

5 **[0108]** For example, as shown in FIG. 4, S12x includes S12x1 and S12x2. It can be understood that, S12x1 and S12x2 can be performed simultaneously, or can be performed sequentially. This is not limited in this specification.

[0109] S12x1: The control device sends the current model parameter #n to the first participating device, and correspondingly, the first participating device receives the current model
10 parameter #n.

[0110] S12x2: The control device sends the current model parameter #n to the second participating device, and correspondingly, the second participating device receives the current model parameter #n.

[0111] S13x: Each of the M participating devices determines intermediate training information
15 #n based on the current model parameter #n and the local dataset.

[0112] The current model parameter #n can be understood as the current model parameter of the risk control model in the process of the n^{th} iteration. The intermediate training information #n is understood as intermediate training information obtained by the participating device in the process of the n^{th} iteration, and the intermediate training information #n obtained by each
20 participating device in the process of the n^{th} iteration is different.

[0113] For example, as shown in FIG. 4, S13x includes S13x1 and S13x2.

[0114] S13x1: The first participating device determines intermediate training information #na based on the current model parameter #n and the local dataset #na.

[0115] A manner in which the first participating device determines the intermediate training
25 information #na is similar to a manner of determining the intermediate training information #1a. For details, references can be made to the above-mentioned descriptions. Details are not described again.

[0116] S13x2: The second participating device determines intermediate training information #nb based on the current model parameter #n and the local dataset #nb.

30 **[0117]** A manner in which the second participating device determines the intermediate training information #nb is similar to a manner of determining the intermediate training information #1b.

For details, references can be made to the above-mentioned descriptions. Details are not described again.

[0118] S14x: The M participating devices each send, to the control device, the intermediate training information #n obtained by each of the M participating devices.

5 [0119] For example, as shown in FIG. 4, S14x includes S14x1 and S14x2.

[0120] S14x1: The first participating device sends the intermediate training information #na to the control device, and correspondingly, the control device receives the intermediate training information #na.

10 [0121] It can be understood that S14x1 and S1401 are similar. For related content and implementations, references can be made to descriptions in S1401. Details are not described again.

[0122] S14x2: The second participating device sends the intermediate training information #nb to the control device, and correspondingly, the control device receives the intermediate training information #nb.

15 [0123] It can be understood that S14x2 and S1402 are similar. For related content and implementations, references can be made to descriptions in S1402. Details are not described again.

[0124] S15x: The control device updates the current model parameter #n of the risk control model based on the M pieces of intermediate training information #n, to obtain a current model parameter #n+1.

20 [0125] It can be understood that S15x and S150 are similar. For related content and implementations, references can be made to descriptions in S150. Details are not described again.

[0126] After obtaining the current model parameter #n+1, the control device determines, based on the training end condition in the above-mentioned example, whether the risk control model corresponding to the current model parameter #n+1 satisfies a requirement. If it is determined that the risk control model corresponding to the current model parameter #n+1 satisfies the requirement, the control device does not need to continue training, and the current model parameter #n+1 is used as the target parameter of the risk control model.

[0127] The method P100 further includes:

[0128] S160: The control device sends the target parameter of the risk control model to each of the M participating devices.

30 [0129] For example, as shown in FIG. 4, S160 includes S1601 and S1602. It can be understood that, S1601 and S1602 can be performed simultaneously, or can be performed sequentially. This

is not limited in this specification.

[0130] S1601: The control device sends the target parameter to the first participating device, and correspondingly, the first participating device receives the target parameter.

[0131] S1602: The control device sends the target parameter to the second participating device, and correspondingly, the second participating device receives the target parameter.

[0132] So far, joint training ends. The target parameter is the risk control model that can identify the risk user and that is obtained after joint training ends.

[0133] It should be noted that, in some application scenarios, it is possible that one of S1601 and S1602 is performed. For example, when the first participating device is a service device of the first service platform that develops a service for a relatively long time, and the second participating device is a service device of the second service platform that newly develops a service, the risk control model obtained after training in the method P100 can be used to identify whether a user in the region in which the second participating device is located is a risk user. Therefore, a cold start caused when the second participating device has a relatively small amount of historical prevention and control data in an earlier service period can be avoided. Alternatively, in some application scenarios, it is possible that neither S1601 nor S1602 is performed. In this case, the first participating device or the second participating device can use, as the target parameter of the risk control model, a parameter updated by the first participating device or the second participating device in the process of the n^{th} iteration.

[0134] Specifically, after obtaining the risk control model, the second participating device can deploy the risk control model on the second service platform, to prevent and control a risk user on the second service platform.

[0135] For example, the second participating device deploys the risk control model in a marketing scenario of the second service platform. When a user A initiates a payment event (for example, rights and interests such as a coupon is used for the payment event) in the marketing scenario on the second service platform, the second service platform can mine, based on the N target feature dimensions, a user feature that is of the user A and that is associated with the payment event, and input the obtained user feature into the risk control model, to obtain a prediction result. The second service platform can determine, based on the prediction result, whether the user A is a risk user. For example, the preset result represents a probability that the user A is a risk user. When the probability is less than or equal to a first threshold, the second service platform determines that

the user A is not a risk user; when the probability is greater than the first threshold and is less than or equal to a second threshold, the second threshold is greater than the first threshold, and the second service platform determines that the user A may be a risk user, that is, the second service platform further needs to determine, with reference to another condition, whether the user A is a risk user; and when the probability is greater than the second threshold, the second service platform determines that the user A is a risk user. If the second service platform determines that the user A is not a risk user, the payment event does not need to be intercepted. In other words, the user A is allowed to complete the payment event. If the second service platform determines that the user A is a risk user, the payment event is intercepted. In other words, the user A is not allowed to complete the payment event. Alternatively, an additional verification procedure is added on the second service platform, and the user A completes the payment event after the user A completes the verification procedure.

[0136] It can be understood that FIG. 3 or FIG. 4 shows an example of a training process of the risk control model that identifies the risk user. By analogy, another risk control model can also be trained based on training logic displayed in the method P100. For example, a risk control model that is used to identify a risk user in another scenario is trained in the method P100. In this case, a user feature included in a local dataset in a training process needs to be combined with the another scenario. Alternatively, a risk control model that is used to identify another risk is trained in the method P100. In this case, a risk feature included in a local dataset in a training process is associated with a specific identified risk.

[0137] It can be further understood that, for the marketing scenario, a plurality of risk control models that identify different risk dimensions can be obtained based on the training logic displayed in P100. The plurality of risk control models include a risk control model corresponding to a user risk dimension (that is, the example risk control model that is used to identify the risk user in the method P100). The plurality of risk control models can be jointly used to identify whether the target event in the marketing scenario is a risk event.

[0138] For example, the user A initiates the payment event in the marketing scenario on the second service platform, and the second service platform can determine a risk feature set corresponding to each of the plurality of risk control models. For each risk control model, the second service platform inputs a risk feature set corresponding to the risk control model into the risk control model, to obtain a risk sub-value of the payment event, and by analogy, obtains a

plurality of risk sub-values corresponding to the plurality of risk control models. Further, the second service platform determines a risk value of the payment event based on the plurality of risk sub-values, and when the risk value is greater than or equal to a risk threshold, determines that the payment event is a risk event, and does not allow the user A to complete the payment event; or
5 when the risk value is less than the risk threshold, determines that the payment event is not a risk event, and allows the user A to continue to complete the payment event.

[0139] It should be noted that in the above-mentioned process of describing the method P100, a marketing scenario of a payment platform is used as an example. Therefore, terms, for example, a user feature and a risk label that are included in the local dataset, used in the marketing scenario
10 are used in specific descriptions. If the method P100 is applied to another platform mentioned above, the used terms can be adjusted adaptively. The terms are not enumerated one by one herein.

[0140] In conclusion, in the model training method, the device, and the storage medium that are provided in this specification, a federated system that includes a control device and a plurality of participating devices performs a plurality of times of iterative joint training, to obtain a risk
15 control model that can identify a risk user. In a process of each time of iterative training, the control device performs coordination, to complete training of the risk control model while a local dataset of the participating device is only used locally, thereby facilitating data privacy protection. In addition, training data of joint training comes from the plurality of participating devices. This breaks a data island, and training data is more abundant and comprehensive. Therefore, a
20 generalization capability, adaptability, and risk control accuracy of the risk control model that are obtained according to this solution are better.

[0141] Another aspect of this specification provides a non-transitory storage medium, storing at least one group of executable instructions used to perform model training. When the executable instructions are executed by a processor, the executable instructions instruct the processor to
25 implement the steps of the method P100 described in this specification. In some possible implementations, aspects of this specification can further be implemented in a form of a program product, including program code. When the program product runs on a control device 100, the program code is used to enable the control device 100 to perform steps performed by the control device 100 in the method P100 described in this specification. When the program product runs on
30 a participating device 200, the program code is used to enable the participating device 200 to perform steps performed by the participating device 200 in the method P100 described in this

specification. When the program product runs on a risk control execution device, the program code is used to enable the risk control execution device to perform the steps of the risk user identification method described in this specification. The program product configured to implement the foregoing method can be a portable compact disk read-only memory (CD-ROM) that includes
5 program code, and can run on the control device 100, the participating device 200, or the risk control execution device. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable
10 medium can be a readable signal medium or a readable storage medium. The readable storage medium can be, for example, an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus, or device, an infrared system, apparatus, or device, or a semiconductor system, apparatus, or device, or any combination thereof. More specific examples of the readable storage medium include: an
15 electrical connection including one or more conducting wires, a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage component, a magnetic storage component, or any proper combination thereof. The computer-readable storage medium can include a data signal propagated
20 in a baseband or as part of a carrier, and carries readable program code. The propagated data signal can be in a plurality of forms, and includes but is not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can further be any readable medium other than the readable storage medium, and the readable medium can be used to send, propagate, or transmit a program used by or in combination with an instruction execution
25 system, apparatus, or component. The program code included in the readable storage medium can be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, optical cable, an RF medium, or any proper combination thereof. Program code for performing an operation of this specification can be written in any combination of one or more program design languages. The program design language includes an object-oriented program
30 design language, for example, Java or C++, and further includes a conventional procedural program design language, for example, "C" language, or a similar program design language. The

program code can be completely executed on the control device 100 and the participating device 200, partially executed on the control device 100 and the participating device 200, executed as an independent software package, partially executed on the control device 100 and the participating device 200 and partially executed on a remote computing device, or completely executed on a remote computing device. The program code can be completely executed on the risk control execution device, partially executed on the risk control execution device, executed as an independent software package, partially executed on the risk control execution device and partially executed on a remote computing device, or completely executed on a remote computing device.

5

[0142] In the technical solutions provided in this specification, collection of related platform data and information transmission between a control device and a participating device comply with provisions of related laws and regulations, and do not violate public order and good morals.

10

[0143] "Plurality of" mentioned in this specification shall be understood as two or more unless otherwise specified.

[0144] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

15

[0145] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the detailed disclosure can be presented only in an example manner, and can impose no limitation. Although it is not explicitly stated here, a person skilled in the art can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be presented in this specification, and fall within the spirit and scope of the example embodiments of this specification.

20

25

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, 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; 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.

2. The method according to claim 1, 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, and the first local dataset comprises a user feature of a first sample user in a region in which the first participating device is located and a risk label of the first sample user;

the second participating device stores a second local dataset, and the second local dataset comprises a user feature of a second sample user in a region in which the second participating device is located; and

the trained risk control model is used to identify whether a user in the region in which the second participating device is located is a risk user.

3. 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.

4. The method according to claim 3, 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.

5. 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.

6. The method according to claim 5, 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.

7. 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.

8. 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.

9. 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, and the method is applied to the 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; 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.

10. The method according to claim 9, 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, and the first local dataset comprises a user feature of a first sample user in a region in which the first participating device is located and a risk label of the first sample user;

the second participating device stores a second local dataset, and the second local dataset comprises a user feature of a second sample user in a region in which the second participating device is located; and

the trained risk control model is used to identify whether a user in the region in which the

second participating device is located is a risk user.

11. The method according to claim 9, 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
5 equal to 1; and

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

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

10 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.

13. The method according to claim 9, wherein the determining intermediate training information based on the current model parameter and the local dataset corresponding to the participating device comprises:

15 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

20 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.

14. The method according to claim 13, wherein the method further comprises:

25 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.

15. The method according to claim 9, wherein the sending the intermediate training information to the control device comprises:

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

sending the ciphertext to the control device.

16. The method according to claim 9, 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.

5 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, and
10 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:

15 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,
20 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; and

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

18. The electronic device according to claim 17, 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
30 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.

19. 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
5 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, and the electronic device serves as one of the M participating devices, 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,
10 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
15 information represents a risk prediction status of the risk control model for the sample user in the local dataset; 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.

20 20. 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 9 is implemented, or the method according to any one of claims 10 to 16 is implemented.