

DESCRIPTION

TITLE:

METHOD AND SYSTEM FOR CONTROLLING USAGE PERMISSION OF TRAINING

5

DATA

BACKGROUND

Technical Field

10 **[0001]** The disclosure relates to a method and system for controlling a usage permission of training data.

Description of Related Art

[0002] With the continuous advancement of artificial intelligence technology, the use of artificial intelligence models to assist in executing automated behaviors such as image
15 detection, image generation, semantic analysis, or intelligent control has become increasingly common. During the construction phase of artificial intelligence models, developers need to use a large amount of training data to train the artificial intelligence models, so as to improve the working performance of the artificial intelligence models.

[0003] However, if the source or acquisition of the aforementioned training data cannot be
20 effectively controlled, disputes related to the ownership of the training data used may easily occur in the subsequent process of using the artificial intelligence models.

SUMMARY

[0004] The disclosure provides a method and system for controlling a usage permission of
25 training data capable of solving the abovementioned problems.

[0005] An embodiment of the disclosure provides a method for controlling a usage permission of training data, and the method includes the following steps. Source verification information corresponding to first training data is obtained. A source of the first training data is confirmed based on the source verification information. If the source of the first training data meets a predetermined condition, a usage permission corresponding to the first training data is enabled, and a computing model is trained based on the first training data. If the source of the first training data does not meet the predetermined condition, the usage permission corresponding to the first training data is disabled.

[0006] An embodiment of the disclosure further provides a system for controlling a usage permission of training data, and the system includes a communication circuit, a storage circuit, and a processor. The storage circuit is configured to store a computing model. The processor is coupled to the communication circuit and the storage circuit. The processor is configured to obtain, through the communication circuit, source verification information corresponding to first training data, confirm a source of the first training data based on the source verification information, enable the usage permission corresponding to the first training data if the source of the first training data meets a predetermined condition and train the computing model based on the first training data, and disable the usage permission corresponding to the first training data if the source of the first training data does not meet the predetermined condition.

[0007] Based on the above, after obtaining the source verification information corresponding to the first training data, the system automatically confirms the source of the first training data based on the source verification information. If the confirmation result reflects that the source of the first training data meets the predetermined condition, the system automatically enables the usage permission corresponding to the first training data and trains the computing model based on the first training data. However, if the confirmation result reflects that the source of the first training data does not meet the predetermined condition, the system disables the usage

permission corresponding to the first training data. In other words, the system automatically controls the usage permission of the training data according to the source of the training data, and in this way, disputes that may arise in the future due to unclear sources of training data or using unauthorized training data to train the computing model are effectively lowered.

5 **[0008]** To make the aforementioned more comprehensible, several embodiments accompanied with drawings are described in detail as follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The accompanying drawings are included to provide a further understanding of the
10 disclosure, and are incorporated in and constitute a part of this specification. The drawings illustrate exemplary embodiments of the disclosure and, together with the description, serve to explain the principles of the disclosure.

[0010] FIG. 1 is a schematic view illustrating a system for controlling a usage permission of training data according to an embodiment of the disclosure.

15 **[0011]** FIG. 2 is a schematic view illustrating execution of controlling the usage permission of the training data based on a block chain network to an embodiment of the disclosure.

[0012] FIG. 3 is a schematic view illustrating execution of controlling the usage permission of the training data according to an embodiment of the disclosure.

[0013] FIG. 4 is a flow chart illustrating a method for controlling a usage permission of
20 training data according to an embodiment of the disclosure.

DESCRIPTION OF THE EMBODIMENTS

[0014] FIG. 1 is a schematic view illustrating a system for controlling a usage permission of training data according to an embodiment of the disclosure. Referring to FIG. 1, a system (also
25 referred to as a system for controlling a usage permission of training data) 10 may be

implemented in various electronic apparatuses with communication and data processing functions, such as Smartphones, tablet computers, laptop computers, desktop computers, servers, or industrial computers, and the types of the electronic apparatuses are not limited to herein.

5 **[0015]** The system 10 includes a communication circuit 11, a storage circuit 12, and a processor 13. The communication circuit 11 is configured to execute wired or wireless communication functions to transmit a signal through wired or wireless methods. For example, the communication circuit 11 may include a communication interface card (such as a network interface card). The communication circuit 11 may support wireless communication standards
10 such as WiFi, Bluetooth, near-field communication (NFC), 3G, 4G, or 5G, or wired communication standards such as Ethernet to transmit a signal. Alternatively, the communication circuit 11 may also support other communication standards, which is not limited by the disclosure. However, the disclosure does not limit the number and type of the communication circuit 11.

15 **[0016]** The storage circuit 12 is configured to store data. For instance, the storage circuit 12 may include a volatile storage circuit and a non-volatile storage circuit. The volatile storage circuit is used to volatily store data. For instance, the volatile storage circuit may include random access memory (RAM) or similar volatile storage media. The non-volatile storage circuit is used to non-volatily store data. For instance, the non-volatile storage circuit may
20 include a read only memory (ROM), a solid state disk (SSD), a conventional hard disk drive (HDD), or similar non-volatile storage media. However, the disclosure does not limit the number and type of the storage circuit 12.

[0017] The processor 13 is coupled to the communication circuit 11 and the storage circuit 12. The processor 13 is used to be responsible for the overall or partial operation of the system
25 10. For instance, the processor 13 may include a central processing unit (CPU), a graphic

processing unit (GPU), a programmable microprocessor for general or special use, a digital signal processor (DSP), a programmable controller, an application specific integrated circuit (ASIC), a programmable logic device (PLD), other similar devices, or a combination of the foregoing devices.

5 **[0018]** In an embodiment, the processor 13 may also include a specialized processor to assist in executing logical operations (such as neural network computation and/or image processing), such as a vision processing unit (VPU), a neural network processing unit (NPU), and/or a tensor processing unit (TPU). However, the disclosure does not limit the number and type of the processor 13.

10 **[0019]** In an embodiment, the system 10 may also include a power management circuit, various input/output devices or peripheral devices such as a mouse, a keyboard, a display, a speaker, and/or a microphone, and the types of input/output interfaces and peripheral devices are not limited herein.

15 **[0020]** In an embodiment, the storage circuit 12 stores a computing model 101. The computing model 101 may be used to execute logical operations (such as neural network computation and/or image processing). For instance, the computing model 101 may use a convolutional neural network (CNN), a recurrent neural network (RNN), a long short term memory (LSTM) model, a deep neural network (DNN), or other types of logical computation architectures to implement the required functions. However, the disclosure does not limit the
20 number and type of the computing model 101.

25 **[0021]** In an embodiment, the processor 13 may obtain verification information (also referred to as source verification information) corresponding to specific training data (also referred to as first training data). The processor 13 may confirm a source of the first training data based on this source verification information. Specifically, if a confirmation result for the source of the first training data reflects that the source of the first training data meets a specific condition

(also referred to as a predetermined condition), the processor 13 may automatically enable a usage permission corresponding to the first training data.

[0022] In an embodiment, when the usage permission corresponding to the first training data is enabled, the processor 13 may (be allowed to) train the computing model 101 based on the first training data. For instance, when the usage permission corresponding to the first training data is enabled, the processor 13 may add the first training data to a training data set corresponding to the computing model 101. The processor 13 may input training data (including the first training data) from the training data set one by one into the computing model 101 and use verification data corresponding to each training data to verify output of the computing model 101. Next, the processor 13 may adjust at least some parameters (such as a weight parameter) used by the computing model 101 according to a verification result (such as a difference between the output of the computing model 101 and the verification data). Therefore, through using the first training data to train the computing model 101, computation performance of the computing model 101 may be improved.

[0023] In an embodiment, if the confirmation result reflects that the source of the first training data does not meet the predetermined condition, the processor 13 may disable the usage permission corresponding to the first training data. Specifically, if the usage permission corresponding to the first training data is not enabled, the processor 13 may not (be allowed to) train the computing model 101 based on the first training data. In an embodiment, if the usage permission corresponding to the first training data is not enabled, the processor 13 may also prohibit training the computing model 101 based on the first training data.

[0024] From another perspective, in an embodiment, the processor 13 only allows the use of the first training data to train the computing model 101 in a situation where the usage permission corresponding to the first training data has been enabled (that is, the source of the first training data meets the predetermined condition). In this way, disputes that may arise in

the future due to unclear sources of training data or using unauthorized training data to train the computing model 101 may be effectively lowered.

[0025] In an embodiment, the processor 13 may obtain information related to the source of the first training data based on the source verification information. For instance, this information may reflect a user name and/or an organization name of a provider of the first training data, upload time of the first training data, an upload location of the first training data, an Internet protocol (IP) address of an upload device (also referred to as a first remote device) of the first training data, a name of the first remote device and/or a type of the first remote device, etc. The processor 13 may then confirm the source of the first training data based on this information.

[0026] In an embodiment, after confirming the source of the first training data, the processor 13 may determine whether the source of the first training data meets the predetermined condition. For instance, it is assumed that a current filtering condition (i.e., the predetermined condition) set for the training data is that a personnel or an organization uploading the training data (i.e., a provider of the training data) must be a personnel or an organization that meet a specific condition (also referred to as a target user). In this situation, the processor 13 may determine whether the source of the first training data is the target user. If the source of the first training data is the target user, the processor 13 may determine that the source of the first training data meets the predetermined condition. However, if the source of the first training data is not the target user, the processor 13 may determine that the source of the first training data does not meet the predetermined condition. It should be noted that the filtering condition (i.e., the predetermined condition) may be adjusted according to practical needs, which is not limited by the disclosure.

[0027] In an embodiment, the provider of the first training data may upload the source verification information corresponding to the first training data to a block chain network in

advance. For instance, the source verification information corresponding to the first training data may be attached to a block chain transaction (also referred to as a first transaction) and uploaded to the block chain network through this transaction (i.e., the first transaction). Afterwards, the processor 13 may get the source verification information from the block chain network.

[0028] In an embodiment, after obtaining the source verification information from the block chain network, the processor 13 may confirm whether the source of the first training data meets the predetermined condition based on block chain verification technology. For instance, according to the block chain verification technology, the processor 13 may confirm whether the transaction (i.e., the first transaction) carrying the source verification information in the block chain network is published by the target user. If the first transaction is published by the target user, the processor 13 may determine that the source of the first training data meets the predetermined condition. Next, the processor 13 may enable the usage permission corresponding to the first training data. However, if the first transaction is not published by the target user, the processor 13 may determine that the source of the first training data does not meet the predetermined condition.

[0029] In an embodiment, if the usage permission corresponding to the first training data is enabled, the processor 13 may further obtain a transaction record (also referred to as a first transaction record) corresponding to the first training data from the block chain network. For instance, the processor 13 may obtain the first transaction record from the first transaction. After obtaining the first transaction record, the processor 13 may obtain location information (also referred to as storage location information) corresponding to the first training data from the first transaction record. For instance, this storage location information may be stored in a form of a uniform resource identifier (URI) or other forms in the first transaction record. Next, the processor 13 may download the first training data from a cloud storage according to this

storage location information.

[0030] In an embodiment, the cloud storage may include a cloud storage provided by major cloud service providers (e.g., Google, Microsoft, or Amazon, etc.) or a cloud storage maintained and/or controlled by any individual, organization, or group. The provider of the first training data may upload the first training data to the cloud storage for storage in advance.

[0031] In an embodiment, the storage location information may point to a resource address in the cloud storage for storing or downloading the first training data. According to the storage location information, the processor 13 may download the first training data from this resource address.

[0032] FIG. 2 is a schematic view illustrating execution of controlling the usage permission of the training data based on a block chain network to an embodiment of the disclosure. Referring to FIG. 2, it is assumed that a plurality of pieces of training data 201(1) to 201(n) are stored in a cloud storage 21. The training data 201(1) to 201(n) may include image data, text data, audio data, or other types of data, as long as they can be used for model training. In an embodiment, it is assumed that the training data 201(i) is the first training data. For instance, the training data 201(i) is uploaded to the cloud storage 21 by a specific user through the first remote device.

[0033] In an embodiment, before or after the specific user uploads the training data 201(i) to the cloud storage 21, the specific user may further create a transaction 202(i) (i.e., the first transaction) in a block chain network 22 through the first remote device. Specifically, the specific user may attach the storage location information corresponding to the training data 201(i) to the transaction 202(i) through the first remote device and publish the transaction 202(i) to the block chain network 22. For instance, after the transaction 202(i) is published to the block chain network 22, the transaction 202(i) may be linked to transactions 202(1) to 202(m) in the block chain network 22.

[0034] In an embodiment, the processor 13 may identify the transaction 202(i) from the block chain network 22 through the communication circuit 11. For instance, the processor 13 may identify the transaction 202(i) from the block chain network 22 by referencing transaction information provided by the specific user. The processor 13 may then parse the transaction 202(i) based on the block chain verification technology to confirm whether the transaction 202(i) is published by the target user. In response to the transaction 202(i) being published by the target user, the processor 13 may determine that a source of the training data 201(i) meets the predetermined condition. The processor 13 may then enable the usage permission corresponding to the training data 201(i). However, if the transaction 202(i) is not published by the target user (i.e., the user who publishes the transaction 202(i) is not the target user), the processor 13 may determine that the source of the training data 201(i) does not meet the predetermined condition. If the source of the training data 201(i) does not meet the predetermined condition, the processor 13 may disable the usage permission corresponding to the training data 201(i).

[0035] In an embodiment, after enabling the usage permission corresponding to the training data 201(i), the processor 13 may further obtain the storage location information corresponding to the training data 201(i) from a transaction record (i.e., the first transaction record) of the transaction 202(i). For instance, this storage location information may be stored in the form of a uniform resource identifier (URI) or other forms in the transaction 202(i). For instance, this storage location information may point to a resource address in the cloud storage 21 for storing or downloading the training data 201(i). According to this storage location information, the processor 13 may download the training data 201(i) from the resource address in the cloud storage 21 through the communication circuit 11. The processor 13 may then use the training data 201(i) to train the computing model 101 of FIG. 1.

[0036] It should be noted that in another embodiment of FIG. 2, in the situation where the

usage permission corresponding to the training data 201(i) is disabled, the processor 13 may not download the training data 201(i) from the cloud storage 21, and even more so may not use the training data 201(i) to train the computing model 101 of FIG. 1. In this way, subsequent disputes related to the ownership of the training data used may be avoided, and the legal usage permission for the training data may be ensured.

[0037] In an embodiment, the provider of the first training data may also upload the source verification information corresponding to the first training data to the cloud storage in advance. Afterwards, the processor 13 may obtain the source verification information from the cloud storage.

[0038] In an embodiment, after obtaining the source verification information from the cloud storage, the processor 13 may confirm the source of the first training data based on digital verification technology. For instance, the digital verification technology may include digital signature technology or any digital analysis technology that can be used for identity verification.

[0039] Taking the digital signature technology as an example, after obtaining the source verification information from the cloud storage, the processor 13 may determine whether the source verification information is signed by the target user based on the digital signature technology. If the source verification information is indeed signed by the target user, the processor 13 may confirm that the source of the first training data meets the predetermined condition. Next, the processor 13 may enable the usage permission corresponding to the first training data. Alternatively, if the source verification information is not signed by the target user, the processor 13 may confirm that the source of the first training data does not meet the predetermined condition.

[0040] In an embodiment, the source verification information may also be information recording the provider of the first training data in a plain or coded form. The processor 13 may

confirm whether the source of the first training data meets the predetermined condition according to the source verification information. For instance, if the source verification information records in a plain or coded form that the provider of the first training data is the target user, then the processor 13 (after executing relevant decoding procedures on the source verification information) may determine that the source of the first training data meets the predetermined condition. Next, the processor 13 may enable the usage permission corresponding to the first training data. Alternatively, if the source verification information records in a plain or coded form that the provider of the first training data is not the target user, then the processor 13 (after executing relevant decoding procedures on the source verification information) may determine that the source of the first training data does not meet the predetermined condition.

[0041] In an embodiment, if the usage permission corresponding to the first training data is enabled, the processor 13 may further obtain the storage location information corresponding to the first training data from a resource list. For instance, the resource list may be provided in advance by the provider of the first training data. For instance, this storage location information may be stored in the form of a uniform resource identifier (URI) or other forms in this resource list. The processor 13 may then download the first training data from the cloud storage according to this storage location information.

[0042] FIG. 3 is a schematic view illustrating execution of controlling the usage permission of the training data according to an embodiment of the disclosure. Referring to FIG. 3, it is assumed that a plurality of pieces of training data 301(1) to 301(n) are stored in a cloud storage 31. The training data 301(1) to 301(n) may include image data, text data, audio data, or other types of data, as long as they can be used for model training. It should be noted that compared to the embodiment of FIG. 2, in the embodiment of FIG. 3, source verification information 302(1) to 302(n) corresponding to the training data 301(1) to 301(n) is also stored in the cloud

storage 31.

[0043] In an embodiment, the training data 301(i) is the first training data, and the source verification information 302(i) is the source verification information corresponding to the first training data. For instance, both the training data 301(i) and the source verification information 302(i) are uploaded to the cloud storage 31 by a specific user through the first remote device.

[0044] In an embodiment, the specific user may provide a resource list 32 through the first remote device. For instance, the resource list 32 may be used to record storage location information corresponding to the training data 301(i) and the source verification information 302(i). For instance, the storage location information may be stored in the resource list 32 in the form of a uniform resource identifier (URI) or other forms. For instance, the storage location information may point to a resource address in the cloud storage 31 for storing or downloading the training data 301(i) and the source verification information 302(i).

[0045] In an embodiment, the processor 13 may obtain the storage location information corresponding to the source verification information 302(i) from the resource list 32.

According to this storage location information, the processor 13 may obtain the source verification information 302(i) from the cloud storage 31 through the communication circuit 11. The processor 13 may determine whether a source of the training data 301(i) meets the predetermined condition according to the source verification information 302(i). For instance, the processor 13 may parse the source verification information 302(i) based on the digital signature technology or other types of digital verification technology to confirm the source of the training data 301(i). Alternatively, if the source verification information 302(i) records the information of the provider of the training data 301(i) in a plain or coded form, the processor 13 may directly confirm the source of the training data 301(i) according to the source verification information 302(i). If the source of the training data 301(i) meets the predetermined condition, the processor 13 may enable the usage permission corresponding to

the training data 301(i). However, if the source of the training data 301(i) does not meet the predetermined condition, the processor 13 may disable the usage permission corresponding to the training data 301(i).

[0046] In an embodiment, after enabling the usage permission corresponding to the training data 301(i), the processor 13 may obtain the storage location information corresponding to the training data 301(i) from the resource list 32. According to this storage location information, the processor 13 may download the training data 301(i) from the cloud storage 31 through the communication circuit 11. The processor 13 may then use the training data 301(i) to train the computing model 101 of FIG. 1.

[0047] It should be noted that in another embodiment of FIG. 3, in the situation where the usage permission corresponding to the training data 301(i) is disabled, the processor 13 may not download the training data 301(i) from the cloud storage 31, and even more so may not use the training data 301(i) to train the computing model 101 of FIG. 1. In this way, subsequent disputes related to the ownership of the training data used may be avoided, and the legal usage permission for the training data may be ensured.

[0048] In an embodiment, the first training data uploaded to the cloud storage by a specific user through the first remote device is processed by compression or encryption. In this way, theft of the first training data can be avoided, and/or the data size of the first training data may be reduced.

[0049] In an embodiment, the first remote device may execute hash encoding or other types of encoding on the first training data to be uploaded, so as to generate an identifier corresponding to the first training data. This identifier may uniquely represent the first training data. That is, the identifiers generated for different training data must be (or have a high probability of being) different. This identifier may then be stored in the cloud storage.

[0050] Thereafter, whenever a new piece of training data (e.g., the first training data) is to be

uploaded to the cloud storage, the first remote device may compare the identifier corresponding to this new training data with the identifiers stored in the cloud storage. If the same identifier already exists in the cloud storage (that is, the identifier corresponding to this new training data is identical to a previously generated identifier), the first remote device may send a notification to remind the provider of the training data that the same training data is already stored in the cloud storage, and repeated uploading is not necessary. In this way, the usage of cloud storage can be effectively saved, and the training data is protected from ownership theft by others.

[0051] FIG. 4 is a flow chart illustrating a method for controlling a usage permission of training data according to an embodiment of the disclosure. Referring to FIG. 4, in step S401, source verification information corresponding to first training data is obtained. In step S402, a source of the first training data is confirmed based on the source verification information. In step S403, it is determined whether the source of the first training data meets a predetermined condition. If the source of the first training data meets the predetermined condition, in step S404, the usage permission corresponding to the first training data is enabled. In step S405, a computing model is trained based on the first training data. However, if the source of the first training data does not meet the predetermined condition, in step S406, the usage permission corresponding to the first training data is disabled.

[0052] Each step of FIG. 4 is described in detail in the foregoing paragraphs, so description thereof is not repeated herein. It should be noted that each step in FIG. 4 may be implemented as a plurality of program codes or circuits, which is not particularly limited by the disclosure. In addition, the method of FIG. 4 may be used in combination with the above-described exemplary embodiments or may be used solely, which is not particularly limited by the disclosure.

[0053] In view of the foregoing, in the method and system for controlling the usage permission of the training data provided by the disclosure, the usage permission of the training

data may be automatically controlled according to the source of the training data. In this way, disputes that may arise in the future due to unclear sources of training data or using unauthorized training data to train the computing model 101 may be effectively lowered, and the legal usage permission for the training data may further be ensured.

- 5 **[0054]** It will be apparent to those skilled in the art that various modifications and variations can be made to the disclosed embodiments without departing from the scope or spirit of the disclosure. In view of the foregoing, it is intended that the disclosure covers modifications and variations provided that they fall within the scope of the following claims and their equivalents.

CLAIMS

Claim 1:

A method for controlling a usage permission of training data, comprising:

obtaining source verification information corresponding to first training data;

5 confirming a source of the first training data based on the source verification information;

enabling a usage permission corresponding to the first training data if the source of the first training data meets a predetermined condition and training a computing model based on the first training data; and

10 disabling the usage permission corresponding to the first training data if the source of the first training data does not meet the predetermined condition.

Claim 2:

The method for controlling the usage permission of the training data according to claim 1, further comprising:

15 allowing the first training data to be used to train the computing model only when the usage permission corresponding to the first training data is enabled.

Claim 3:

20 The method for controlling the usage permission of the training data according to claim 1, wherein the source verification information is obtained from a block chain network, and the step of confirming the source of the first training data based on the source verification information comprises:

confirming whether the source of the first training data meets the predetermined condition based on block chain verification technology.

25

Claim 4:

The method for controlling the usage permission of the training data according to claim 3, further comprising:

obtaining a transaction record corresponding to the first training data from the block chain network after enabling the usage permission corresponding to the first training data;

obtaining storage location information corresponding to the first training data from the transaction record; and

downloading the first training data from a cloud storage according to the storage location information.

Claim 5:

The method for controlling the usage permission of the training data according to claim 4, wherein the storage location information is stored in a form of a uniform resource identifier in the transaction record.

Claim 6:

The method for controlling the usage permission of the training data according to claim 1, wherein the source verification information is obtained from a cloud storage, and the step of confirming the source of the first training data based on the source verification information comprises:

confirming whether the source of the first training data meets the predetermined condition based on digital verification technology.

Claim 7:

The method for controlling the usage permission of the training data according to claim 6,

further comprising:

obtaining storage location information corresponding to the first training data from a resource list after enabling the usage permission corresponding to the first training data; and

downloading the first training data from the cloud storage according to the storage location

5 information.

Claim 8:

A system for controlling a usage permission of training data, comprising:

a communication circuit;

10 a storage circuit configured to store a computing model; and

a processor coupled to the communication circuit and the storage circuit,

wherein the processor is configured to:

obtain, through the communication circuit, source verification information corresponding to first training data,

15 confirm a source of the first training data based on the source verification information,

enable the usage permission corresponding to the first training data if the source of the first training data meets a predetermined condition and train the computing model based on the first training data, and

20 disable the usage permission corresponding to the first training data if the source of the first training data does not meet the predetermined condition.

Claim 9:

The system for controlling the usage permission of the training data according to claim 8,

25 wherein the processor is further configured to:

allow the first training data to be used to train the computing model only when the usage permission corresponding to the first training data is enabled.

Claim 10:

5 The system for controlling the usage permission of the training data according to claim 8, wherein the source verification information is obtained from a block chain network, and the operation of confirming, by the processor, the source of the first training data based on the source verification information comprises:

10 confirm whether the source of the first training data meets the predetermined condition based on block chain verification technology.

Claim 11:

10 The system for controlling the usage permission of the training data according to claim 10, wherein the processor is further configured to:

15 obtain a transaction record corresponding to the first training data from the block chain network after enabling the usage permission corresponding to the first training data,

 obtain storage location information corresponding to the first training data from the transaction record, and

20 download the first training data from a cloud storage according to the storage location information.

Claim 12:

 The system for controlling the usage permission of the training data according to claim 11, wherein the storage location information is stored in a form of a uniform resource identifier

25 in the transaction record.

Claim 13:

The system for controlling the usage permission of the training data according to claim 8,
wherein the source verification information is obtained from a cloud storage, and the operation
5 of confirming, by the processor, the source of the first training data based on the source
verification information comprises:

confirm whether the source of the first training data meets the predetermined condition
based on digital verification technology.

10 Claim 14:

The system for controlling the usage permission of the training data according to claim
13, wherein the processor is further configured to:

obtain storage location information corresponding to the first training data from a resource
list after enabling the usage permission corresponding to the first training data, and

15 download the first training data from the cloud storage according to the storage location
information.