CLAIMS

What is claimed is:

1. A risk identification method for identifying a false transaction~~training a risk identification model~~, comprising:

a method for training risk identification model, the method comprises:

determining a type of a target unsupervised machine learning algorithm;

extracting feature information from input information, and extracting target feature information from the feature information in a way of extracting feature information corresponding to the type of the target unsupervised machine learning algorithm; and

obtaining a target risk identification model corresponding to the target unsupervised machine learning algorithm by training a risk identification model using the target feature information and the target unsupervised machine learning algorithm;

obtaining a plurality of target risk identification models, wherein the plurality of target risk identification models are trained using the method for training a risk identification model;

determining a first risk identification model having identification accuracy meeting predetermined threshold from the plurality of target risk identification models; and

performing risk identification on a new sample based on the first risk identification model to obtain a risk identification result, wherein the risk identification result provides an indication on whether the new sample is the false transaction.

2. The risk identification method according to claim 1, wherein the input information includes one or more of user profile information, historical transaction information, device medium information, geographical location information, address book information, or external information.

3. The risk identification method according to claim 2, wherein the feature information includes one or more of frequency feature information, location feature information, graph feature information and behavior sequence feature information in the input information.

4. The risk identification method according to claim 1, wherein the extracting the target feature information from the feature information in the way of extracting feature information corresponding to the type of the target unsupervised machine learning algorithm includes:

determining a key performance indicator value of each piece of feature information in response to that the type is a tree-based unsupervised machine learning type; and

extracting, based on the key performance indicator value of each piece of feature information, target feature information from the feature information based on a preset policy.

5. The risk identification method according to claim 4, wherein the extracting, based on the key performance indicator value of each piece of feature information, the target feature information from the feature information based on the preset policy includes:

determining feature information having key performance indicator value that meets a preset relationship with a preset performance indicator value as the target feature information; or

ranking, based on the key performance indicator value of each piece of feature information, the feature information in a predetermined way, and determining feature information that is ranked before a predetermined ranking place as the target feature information.

6. The risk identification method according to claim 4, wherein the key performance indicator value includes one or more of a kurtosis value or a dispersion value.

7. The risk identification method according to claim 1, wherein the extracting the target feature information from the feature information in the way of extracting feature information corresponding to the type of the target unsupervised machine learning algorithm includes:

performing dimensionality reduction transformation on the feature information to obtain target feature information in response to that the type is a distance-based unsupervised machine learning type.

~~8. A risk identification method, comprising:~~

~~obtaining a plurality of target risk identification models corresponding to a plurality of target unsupervised machine learning algorithms by performing model training using a method according to any one of claims 1 to 7;~~

~~determining a first risk identification model having identification accuracy meeting a predetermined threshold from the plurality of target risk identification models; and~~

~~performing risk identification on new samples based on the first risk identification model to obtain a risk identification result.~~

8~~9~~. A~~n~~ risk identification apparatus for identifying a false transaction~~training a risk identification model~~, comprising:

an apparatus for training a risk identification model, the apparatus comprises:

a determining unit, configured to determine a type of a target unsupervised machine learning algorithm;

a feature extraction unit, configured to extract feature information from input information, and extract target feature information from the feature information in a way of extracting feature information corresponding to the type of the target unsupervised machine learning algorithm; and

a training unit, configured to obtain a target risk identification model corresponding to the target unsupervised machine learning algorithm by training a risk identification model using the target feature information and the target unsupervised machine learning algorithm; and

a risk identification unit configured to:

obtain a plurality of target risk identification models trained by the apparatus for training a risk identification model;

determine a first risk identification model having identification accuracy meeting a predetermined threshold from the plurality of target risk identification models; and

perform risk identification on a new sample based on the first risk identification model to obtain a risk identification result, wherein the risk identification result provides an indication on whether the new sample is the false transaction.

9~~10~~. The risk identification apparatus according to claim 8~~9~~, wherein the feature extraction unit is specifically configured to:

determine a key performance indicator value of each piece of feature information in response to that the type is a tree-based unsupervised machine learning type; and

extract, based on the key performance indicator value of each piece of feature information, target feature information from the feature information based on a preset policy.

10~~1~~. The risk identification apparatus according to claim 9~~10~~, wherein the feature extraction unit is specifically configured to:

determine the feature information having key performance indicator value that meets a preset relationship with a preset performance indicator value as the target feature information; or

rank, based on the key performance indicator value of each piece of feature information, the feature information in a predetermined way, and determine the feature information that is ranked before a predetermined ranking place as the target feature information.

11~~2~~. The risk identification apparatus according to claim 8~~9~~, wherein the feature extraction unit is specifically configured to:

perform dimensionality reduction transformation on the feature information to obtain target feature information in response to that the type is a distance-based unsupervised machine learning type.

~~13. A risk identification apparatus, comprising:~~

~~a risk identification unit, configured to, by the apparatus according to any one of claims 9 to 12, train and obtain a plurality of target risk identification models corresponding to a plurality of target unsupervised machine learning algorithms, determine a first risk identification model having identification accuracy meeting a~~

~~predetermined threshold from the plurality of target risk identification models, and perform risk identification on new samples based on the first risk identification model to obtain a risk identification result.~~

124. A server, comprising a memory, a processor, and a computer program stored in the memory and executable on the processor, wherein the processor implements the steps of the risk identification method according to any one of claims 1 to 7~~8~~ when executing the program.

135. A computer-readable storage medium storing a computer program, wherein the steps of the risk identification method according to any one of claims 1 to 7~~8~~ are implemented when the program is executed by a processor.