CLAIMS

What is claimed is:

1. An identity verification method, comprising:

receiving an identity verification request from a to-be-verified device, wherein the identity verification request comprises device environment information of the to-be-verified device, and is used for requesting identity verification of a user corresponding to the to-be-verified device;

determining a credibility of the to-be-verified device according to historical feature information and the device environment information, wherein the historical feature information comprises device environment information of a historical device by:

determining a feature vector corresponding to the to-be-verified device according to the device environment information when a type of information comprised in the device environment information matches a preset information type,

inputting the feature vector to a device verification model, and

determining the credibility of the to-be-verified device by using the device verification model, wherein the device verification model is configured to determine, based on device environment information, a credibility label of a device that sends the identity verification request and a probability that the identity verification request is predicted as a credible request; and

determining, according to the credibility of the to-be-verified device, an identity verification policy for performing identity verification on the user, so as to perform identity verification according to the identity verification policy.

2. The method according to claim 1, wherein before the inputting the feature vector to a device verification model, and determining the credibility of the to-be-verified device by using the device verification model, the method further comprises:

obtaining historical feature information corresponding to the historical device;

determining, according to a time interval corresponding to the historical feature information, a training set comprising first historical feature information and a verification set comprising second historical feature information; and

training the device verification model by using the first historical feature information, and verifying the device verification model by using the second historical feature information.

3. The method according to claim 2, wherein the determining, according to a time interval corresponding to the historical feature information, a training set comprising first historical feature information and a verification set comprising second historical feature information comprises:

according to the time interval corresponding to the historical feature information, assigning first historical feature information generated at an earlier moment to the training set, and assigning second historical feature information generated at a later moment to the verification set.

4. The method according to claim 2, wherein the device verification model comprises an LR (logistic regression) model and an XGBoost (extreme gradient boosting) model, wherein the training the device verification model by using the first historical feature information comprises:

determining, according to the first historical feature information, a first historical feature vector, a second historical feature vector, and a first credibility label of a historical device corresponding to the first historical feature information;

inputting the first historical feature vector to the LR model; adjusting a model parameter of the LR model according to the first credibility label and a first target label output by the LR model until the output of the logistic regression LR model satisfies a preset condition;

calculating, according to an output of the trained LR model, a first probability that an identity verification request sent by the device corresponding to the first historical feature information is predicted as a credible request;

inputting the first probability and the second historical feature vector to the XGBoost model; and adjusting a model parameter of the XGBoost model based on an output of the XGBoost model and the first credibility label until the output of the XGBoost model satisfies a preset condition, wherein the output of the XGBoost model comprises the first credibility label of the historical device corresponding to the first historical feature information and a probability that an identity verification request sent by the historical device is predicted as a credible request.

5. The method according to claim 4, wherein the verifying the device verification model by using the second historical feature information comprises:

determining, according to the second historical feature information, a third historical

feature vector, a fourth historical feature vector, and a second credibility label of a historical device corresponding to the second historical feature information;

inputting the third historical feature vector to the trained LR model;

calculating, according to the output of the trained LR model, a second probability that an identity verification request sent by the device corresponding to the second historical feature information is predicted as a credible request;

inputting the second probability and the fourth historical feature vector to the trained XGBoost model, and obtaining an output of the device verification model by using the trained XGBoost model, wherein the output of the device verification model comprises the second credibility label of the historical device corresponding to the second historical feature information and a third probability that an identity verification request sent by the historical device is predicted as a credible request;

obtaining evaluation data of the device verification model by using a binary classification method according to the output of the device verification model and the second credibility label; and

adjusting the model parameter of the LR model and/or the model parameter of the XGBoost model according to the evaluation data until the evaluation data of the device verification model satisfies a preset condition.

6. The method according to claim 5, wherein the evaluation data of the device verification model comprises at least one of an F1 score and an AUC (area under the curve) value.

7. The method according to any of claims 4 to 6, wherein the model parameter of the LR model comprises at least one of: a regularization term, a regularization coefficient, and a maximum iteration number.

8. The method according to any of claims 4 to 6, wherein a number of components in the first historical feature vector is greater than a number of components in the second historical feature vector.

9. The method according to any of claims 1 to 6, wherein the historical device comprises at least one of: a historical login device and a historical identity verification device.

10. The method according to any of claims 1 to 6, wherein the determining a credibility of the to-be-verified device according to historical feature information and the device environment information comprises:

determining that the to-be-verified device is incredible when the type of the information comprised in the device environment information does not match the preset information type.

11. The method according to claim 10, wherein the preset information type comprises at least one of: an identity ID of a device, and a WI-FI connection, an LBS (location-based service), and an IP (Internet Protocol)address corresponding to the device.

12. The method according to any of claims 1 to 6, wherein the determining, according to the credibility of the to-be-verified device, an identity verification policy for performing identity verification on the user comprises:

determining, according to the credibility of the to-be-verified device and a correspondence between the identity verification policy and a credibility interval, the identity verification policy for performing identity verification on the user, wherein:

a risk level matching the identity verification policy is in a negative relationship with a credibility of a user-held device.

13. The method according to claim 12, wherein the identity verification policy comprises at least one of an identity verification information type, an identity verification information amount, and an identity verification threshold range,

wherein the risk level matching the identity verification policy being in a negative relationship with the credibility of the user-held device comprises at least one of the following:

when the identity verification policy comprises the identity verification information type, a security level of the identity verification information type in the identity verification policy is in a negative relationship with the credibility of the user-held device;

when the identity verification policy comprises the identity verification information amount, the identity verification information amount in the identity verification policy is in a negative relationship with the credibility of the user-held device; and

when the identity verification policy comprises the identity verification threshold range, the identity verification threshold range in the identity verification policy is in a positive relationship with the credibility of the user-held device.

14. The method according to claim 1, wherein performing the identity verification according to the identity verification policy comprises:

determining, according to the identity verification policy, an identity verification process, information required for the identity verification, and an identity verification threshold range of the information required for the identity verification;

prompting, according to the identity verification process, the to-be-verified device to report the information required for the identity verification; and

when receiving the information required for the identity verification from the to-be-verified device, performing the identity verification according to the identity verification threshold range of the information required for the identity verification.

15. An identity verification apparatus, comprising:

a request receiving module configured to receive an identity verification request from a to-be-verified device, wherein the identity verification request comprises device environment information of the to-be-verified device, and is used for requesting identity verification of a user corresponding to the to-be-verified device;

a credibility determining module configured to determine a credibility of the to-be-verified device according to historical feature information and the device environment information, wherein the historical feature information comprises device environment information of a historical device by:

determining a feature vector corresponding to the to-be-verified device according to the device environment information when a type of information comprised in the device environment information matches a preset information type,

inputting the feature vector to a device verification model, and

determining the credibility of the to-be-verified device by using the device verification model, wherein the device verification model is configured to determine, based on device environment information, a credibility label of a device that sends the identity verification request and a probability that the identity verification request is predicted as a credible request; and

an identity verification policy determining module configured to determine, according to the credibility of the to-be-verified device, an identity verification policy for performing identity verification on the user, so as to perform identity verification according to the identity verification policy.

16. An electronic device, comprising:

a processor; and

a memory configured to store computer executable instructions that when executed, cause the processor to perform operations comprising:

receiving an identity verification request from a to-be-verified device, wherein the identity verification request comprises device environment information of the to-be-verified device, and is used for requesting identity verification of a user corresponding to the to-be-verified device;

determining a credibility of the to-be-verified device according to historical feature information and the device environment information, wherein the historical feature information comprises device environment information of a historical device by:

determining a feature vector corresponding to the to-be-verified device according to the device environment information when a type of information comprised in the device environment information matches a preset information type,

inputting the feature vector to a device verification model, and

determining the credibility of the to-be-verified device by using the device verification model, wherein the device verification model is configured to determine, based on device environment information, a credibility label of a device that sends the identity verification request and a probability that the identity verification request is predicted as a credible request; and

determining, according to the credibility of the to-be-verified device, an identity verification policy for performing identity verification on the user, so as to perform identity verification according to the identity verification policy.

17. A computer readable storage medium storing one or more programs that, when executed by an electronic device comprising a plurality of applications, cause the electronic device to perform operations comprising:

receiving an identity verification request from a to-be-verified device, wherein the identity verification request comprises device environment information of the to-be-verified device, and is used for requesting identity verification of a user corresponding to the to-be-verified device;

determining a credibility of the to-be-verified device according to historical feature information and the device environment information, wherein the historical feature

information comprises device environment information of a historical device by:

determining a feature vector corresponding to the to-be-verified device according to the device environment information when a type of information comprised in the device environment information matches a preset information type,

inputting the feature vector to a device verification model, and

determining the credibility of the to-be-verified device by using the device verification model, wherein the device verification model is configured to determine, based on device environment information, a credibility label of a device that sends the identity verification request and a probability that the identity verification request is predicted as a credible request; and

determining, according to the credibility of the to-be-verified device, an identity verification policy for performing identity verification on the user, so as to perform identity verification according to the identity verification policy.