

IDENTITY VERIFICATION METHOD AND APPARATUS

TECHNICAL FIELD

[0001] The present application relates to the field of computer technologies, and in particular, to an identity verification method and apparatus.

BACKGROUND

[0002] With the popularity of the mobile Internet and the development of mobile payment services, more users use smart terminals for operations such as online shopping and payment.

[0003] In order to protect security of user services and resources, when a user logs into a system or participates in the service, an identity of the user usually needs to be verified to determine whether the user requesting to log into the system or participate in the service has a corresponding authorization, that is, determine whether the user logging into the system is the real user. Therefore, relatively high requirements are imposed on security and reliability of identity verification.

[0004] Therefore, an identity verification method helping improve the security and the reliability of identity verification and satisfying usage requirements of a user is urgently required.

SUMMARY

[0005] Embodiments of the present application provide an identity verification method and apparatus to improve security and reliability of identity verification and satisfy usage requirements of a user.

[0006] The embodiments of the present application adopt the following technical solutions.

[0007] According to a first aspect, an embodiment of the present application provides an identity verification method, including:

[0008] receiving an identity verification request from a to-be-verified device, where the identity verification request includes 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;

[0009] determining a credibility of the to-be-verified device according to historical feature

information and the device environment information, where the historical feature information includes device environment information of a historical device; and

[0010] 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.

[0011] Optionally, in the identity verification method provided in the first aspect, the determining a credibility of the to-be-verified device according to historical feature information and the device environment information includes:

[0012] determining a feature vector corresponding to the to-be-verified device according to the device environment information when a type of information included in the device environment information matches a preset information type; and

[0013] 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, where 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.

[0014] Optionally, in the identity verification method provided in the first aspect, 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 includes:

[0015] obtaining historical feature information corresponding to the historical device;

[0016] 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

[0017] 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.

[0018] Optionally, in the identity verification method provided in the first aspect, 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 includes:

[0019] 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.

[0020] Optionally, in the identity verification method provided in the first aspect, the device verification model includes an LR (logistic regression) model and an XGBoost (extreme gradient boosting) model, where the training the device verification model by using the first historical feature information includes:

[0021] 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;

[0022] 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 LR model satisfies a preset condition;

[0023] 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;

[0024] 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 includes 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.

[0025] Optionally, in the identity verification method provided in the first aspect, the verifying the device verification model by using the second historical feature information includes:

[0026] 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;

[0027] 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;

[0028] 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, where the output of the device verification model includes 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;

[0029] 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

[0030] 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.

[0031] Optionally, in the identity verification method provided in the first aspect, the evaluation data of the device verification model includes at least one of an F1 score and an AUC (area under the curve) value.

[0032] Optionally, in the identity verification method provided in the first aspect, the model parameter of the LR model includes at least one of: a regularization term, a regularization coefficient, and a maximum iteration number.

[0033] Optionally, in the identity verification method provided in the first aspect, a number of components in the first historical feature vector is greater than a number of components in the second historical feature vector.

[0034] Optionally, in the identity verification method provided in the first aspect, the historical device includes at least one of: a historical login device and a historical identity verification device.

[0035] Optionally, in the identity verification method provided in the first aspect, the determining a credibility of the to-be-verified device according to historical feature information and the device environment information includes:

[0036] determining that the to-be-verified device is incredible when the type of the information included in the device environment information does not match the preset information type.

[0037] Optionally, in the identity verification method provided in the first aspect, the preset information type includes at least one of an identity ID of a device, and a wireless connection (Wi-Fi), an LBS (location-based service), and an IP (Internet Protocol) address corresponding to the device.

[0038] Optionally, in the identity verification method provided in the first aspect, the determining, according to the credibility of the to-be-verified device, an identity verification policy for performing identity verification on the user includes:

[0039] 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, where

[0040] a risk level matching the identity verification policy is in a negative relationship with a credibility of a user-held device.

[0041] Optionally, in the identity verification method provided in the first aspect, the identity verification policy includes at least one of an identity verification information type, an identity verification information amount, and an identity verification threshold range,

[0042] wherein the risk level matching the identity verification policy being in a negative relationship with the credibility of the user-held device includes at least one of the following:

[0043] when the identity verification policy includes 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;

[0044] when the identity verification policy includes 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

[0045] when the identity verification policy includes 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.

[0046] Optionally, in the identity verification method provided in the first aspect, performing the identity verification according to the identity verification policy includes:

[0047] 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;

[0048] prompting, according to the identity verification process, the to-be-verified device to report the information required for the identity verification; and

[0049] 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.

[0050] According to a first aspect, an embodiment of the present application provides an identity verification apparatus, including:

[0051] a request receiving module configured to receive an identity verification request from a to-be-verified device, where the identity verification request includes 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;

[0052] 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, where the historical feature information includes device environment information of a historical device; and

[0053] 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.

[0054] According to a first aspect, an embodiment of the present application provides an electronic device, including:

[0055] a processor; and

[0056] a memory configured to store computer executable instructions that when executed, cause the processor to perform operations comprising:

[0057] receiving an identity verification request from a to-be-verified device, where the identity verification request includes 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;

[0058] determining a credibility of the to-be-verified device according to historical feature information and the device environment information, where the historical feature information includes device environment information of a historical device; and

[0059] 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.

[0060] According to a fourth aspect, an embodiment of the present application provides a computer readable storage medium storing one or more programs that, when executed by an electronic device including a plurality of applications, cause the electronic device to perform operations comprising:

[0061] receiving an identity verification request from a to-be-verified device, where the identity verification request includes 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;

[0062] determining a credibility of the to-be-verified device according to historical feature information and the device environment information, where the historical feature information

includes device environment information of a historical device; and

[0063] 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.

[0064] The at least one technical solution adopted in the embodiments of the present application can achieve the following beneficial effects.

[0065] In the embodiments of the present application, after the verification request is received from the to-be-verified device, the verification is not directly performed, but the credibility of the to-be-verified device is determined according to the device environment information of the historical device and the device environment information of the to-be-verified device, and the identity verification policy for performing identity verification on the user is further determined according to the credibility. According to the method in the embodiments of the present application, without awareness of a user, an identity verification policy applicable to a current user-held device can be selected for the user according to the credibility of the user-held device. Therefore, the embodiments of the present application facilitate improvements in the security and the reliability of identity verification, and can satisfy usage requirements of the user, and improve the user experience.

BRIEF DESCRIPTION OF THE DRAWINGS

[0066] The accompanying drawings described herein are used for providing further understanding for the present application and constitute a part of the present application. Exemplary embodiments of the present application and descriptions thereof are used for explaining the present application and do not constitute an improper limitation to the present application. In the accompanying drawings:

[0067] FIG. 1 is a schematic flowchart of an identity verification method, according to an embodiment of the present application;

[0068] FIG. 2 is a second schematic flowchart of an identity verification method, according to an embodiment of the present application;

[0069] FIG. 3 is a third schematic flowchart of an identity verification method, according to an embodiment of the present application;

[0070] FIG. 4 is a fourth schematic flowchart of an identity verification method, according to an embodiment of the present application;

[0071] FIG. 5 is a fifth schematic flowchart of an identity verification method, according

to an embodiment of the present application;

[0072] FIG. 6 is a sixth schematic flowchart of an identity verification method according to an embodiment of the present application;

[0073] FIG. 7 is a schematic structural diagram of an identity verification apparatus, according to an embodiment of the present application; and

[0074] FIG. 8 is a schematic structural diagram of an electronic device, according to an embodiment of the present application.

DETAILED DESCRIPTION OF THE INVENTION

[0075] In order to make the objects, technical solutions, and advantages of the present application more clear, the technical solutions of the present application will be clearly and completely described below in the following with reference to the embodiments of the present application. It is obvious that the embodiments to be described are only some rather than all of the embodiments of the present application. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present application without creative efforts shall fall within the protection scope of the present application.

[0076] In the Internet era, regardless of the mobile Internet or a mobile payment service, an identity of a user accessing a network platform or using a service system needs to be verified, that is, identity checking or identity authentication needs to be performed to ensure security of the network platform and the service system, thereby ensuring that the user accessing the network platform or using the service system has legitimate authorization. During specific implementation, an identity verification system that implements an identity verification function may be either a dedicated identity verification system independent of the service system or a part of the service system.

[0077] During identity verification of a user, information (for example, a login password, a payment password, a fingerprint, etc.) input by the user applying for identity verification to the identity verification system may be compared to information stored in the backend of the identity verification system. When it is determined through comparison that the information satisfies a condition (for example, complete consistency or a deviation within a preset range, etc.), identity verification of the user applying identity verification may be considered to be successful and the user may be considered to have authorization to participate in a service.

[0078] Optionally, a biological recognition technology such as fingerprint recognition, face recognition, voiceprint recognition, iris recognition, etc. may be used for identity

verification. During specific implementation, biological characteristics of the user applying for identity verification may be compared to biological characteristics stored in the backend, and an identity of the user may be verified according to a comparison result.

[0079] Optionally, text message code verification or security question verification may also be used for identity verification. During specific implementation, the identity verification system may provide a randomly generated text message verification code or a preset security question for the user applying for identity verification. After a text message code or an answer to the security question fed back by the user is received, the identity of the user may be verified through determining whether the answer of the user is consistent with a stored answer or a correct answer determined by the identity verification system.

[0080] With the improvement of technical levels, optimizing only one of the above aspects, for example, designing a longer, more complex, and more time-effective password to improve security of password verification, or improving bandwidth and server stability to ensure stability of sending a third-party password (for example, a text message verification code), thereby improving security and reliability of identity verification may have increasing marginal costs.

[0081] In order to improve the security and the reliability of identity verification and meet usage requirements of a user, an embodiment of the present application provides an identity verification method to be performed by the identity verification system. It may be understood that the identity verification system may be independent of the service system or may be used as a part of the service system to implement a function of verifying an identity of a user in a service process. In the verification method provided in this embodiment of the present application, auxiliary verification is performed by using device environment information to determine a potential risk of a user applying for identity verification. For example, a credibility of a device held by the user is determined according to device environment information of the user-held device and device environment information of a historical device, and an identity verification policy for performing identity verification on the user is further determined according to the credibility.

[0082] It should be noted that a higher credibility of the terminal device indicates more reasonable and securer use of the mobile terminal by the user applying for identity verification. Therefore, a relatively moderate identity verification policy matching a relatively low risk level may be used to verify the identity of the user. Correspondingly, a lower credibility of the terminal device indicates less reasonable and less secure use of the mobile terminal by the user applying for identity verification. Therefore, a relatively strict identity

verification policy matching a relatively high risk level needs to be used to verify the identity of the user.

[0083] It may be understood that the terminal device held by the user and the to-be-verified device in this embodiment of the present application may be a device such as a personal computer, or may be a mobile terminal device such as a smartphone or a tablet computer. The terminal device is used by the user for sending an identity verification request and applying for service participation.

[0084] According to the method in this embodiment of the present application, the device core information may be used for assisting identity verification sustainably without awareness of the user. Moreover, a strong verification manner such as biological characteristic verification, security question verification, etc. may be further used, and an identity verification policy suitable for the current user-held device may be selected for the user based on a determined credibility of the user-held device. Optionally, a security verification level of the biological characteristic verification or security question verification may be appropriately adjusted according to the credibility of the device. For example, a higher credibility of the device may indicate a lower comparison threshold during face verification. For another example, a higher credibility of the device may indicate fewer questions during security question verification, and so on.

[0085] Therefore, in the embodiment of the present application, the device environment information is used to assist the identity verification, helping improve security and reliability of the identity verification. In addition, the identity verification policy may be selected according to the credibility of the device, so that user requirements of the user can be better satisfied and user experience can be improved.

[0086] The technical solutions provided in the embodiments of the present application are described in detail below with reference to the drawings.

[0087] Referring to FIG. 1, an embodiment of the present application provides an identity verification method that may be performed by an identity verification system. The method may include the following steps.

[0088] S101: Receive an identity verification request from a to-be-verified device, where the identity verification request includes 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.

[0089] It may be understood that when a user wishes to log into a service system or to initiate a service request in the service system, identity verification usually needs to be

performed first, that is, an identity of the user needs to be verified. The identity verification system executes the identity verification request received in step S101. The identity verification request may be a login request or a service request initiated by the user through a held terminal device, or may be an identity verification request dedicated to request identity verification on the user corresponding to the device.

[0090] Optionally, the device environment information of the to-be-verified device may include an identity ID of the to-be-verified device, an Internet Protocol (IP) address on a network to which the to-be-verified device is connected, etc. For a to-be-verified device connected to a mobile communication network or a wireless network, the device environment information of the to-be-verified device may further include a Wireless-Fidelity (Wi-Fi) connection, a location based service (LBS), etc.

[0091] It may be understood that when the to-be-verified device sends the identity verification request to the identity verification system, the to-be-verified device is certainly connected to the Internet or the mobile Internet. Therefore, the device environment information sent by the to-be-verified device to the identity verification system can reflect the identity of the to-be-verified device (embodied by a carried identity ID) and a network environment authorized to the user when applying for identity verification by using the to-be-verified device, which may be embodied by an IP address, Wi-Fi, an LBS, etc. corresponding to the device.

[0092] S103: Determine a credibility of the to-be-verified device according to historical feature information and the device environment information, where the historical feature information includes device environment information of a historical device.

[0093] After the device environment information of the to-be-verified device is received, the identity verification system further performs step S103 of determining the credibility of the to-be-verified device by using the historical feature information including the device environment information of the to-be-verified device. It may be understood that a particular user usually corresponds to one or more frequently used terminal devices (for example, smartphones, tablet computers, wearable intelligent devices, laptops, etc.) and one or more network environments to which a connection is usually established (for example, a home network, an office network, a frequent shopping mall network, a restaurant network, etc.). These frequently used terminal devices and network environments to which a connection is frequently established may be embodied by the above historical feature information. Therefore, the identity verification system may determine the credibility of the to-be-verified device based on the historical feature information and the device environment information of

the current device applying for identity verification. It may be determined by using the credibility whether applying by the particular user for identity verification through the to-be-verified device is reasonable and consistent with the routine.

[0094] The credibility of the to-be-verified device may be determined according to historical feature information and the device environment information in various manners and by using various specific standards. For example, the identity ID of the to-be-verified device may be compared to an identity ID of the historical device in the historical feature information. If the identities are the same, it may be considered that the to-be-verified device is more likely to be credible. For another example, matching may be performed between a network environment to which the to-be-verified device is connected and a network environment to which the historical device is connected in the historical feature information. If the network environments match each other (for example, the to-be-verified device and the historical device are connected to the same Wi-Fi), it may be considered that the to-be-verified device is more likely to be credible. For still another example, matching may be performed between location information of the to-be-verified device determined based on the LBS and location information of the historical device determined based on the LBS in the historical feature information. If the location information does not match each other (for example, a location of the to-be-verified device does not appear in the historical feature information), it may be considered that the to-be-verified device is more likely to be incredible.

[0095] Optionally, when the identity verification system determines the credibility of the to-be-verified device according to the historical feature information and the device environment information, if a type of information included in the device environment information of the to-be-verified device does not match a preset information type, the identity verification system may directly determine that the to-be-verified device is incredible. It may be understood that the preset information type may include at least one of an identity ID of a device, and a wireless connection (Wi-Fi), a location-based service (LBS), and an Internet Protocol (IP) address corresponding to the device. It should be noted that, since users may use different types of devices that may be connected to different types of network environments, different preset information types are preset for different network environments according to types of information that the devices can have when being normally connected to a network. In this case, if the device environment information sent by the to-be-verified device to the identity verification system lacks information of the type specified in the preset information type, it may be considered that the to-be-verified device is

illegally used, as a result of which device environment information originally required to be reported is shielded to escape from verification by the identity verification system. Therefore, the identity verification system may directly determine that the to-be-verified device is incredible, and then adopts a more strict identity verification policy applicable to a higher risk level for identity verification.

[0096] Optionally, the identity verification may determine the credibility of the to-be-verified device according to the historical feature information and the device environment information by using a device verification model. For example, an input of the device verification model is a feature vector determined according to the device environment information of the to-be-verified device, and output is a credibility label of the to-be-verified device and a probability that the identity verification request sent by the to-be-verified device is predicted as a credible request. Therefore, an identity verification policy for performing identity verification on the user can be determined on this basis.

[0097] A method for constructing and training the device verification model and a specific implementation process of determining the credibility of the to-be-verified device by using the device verification model are described in detail below by using examples.

[0098] S105: 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.

[0099] Optionally, the identity verification policy for performing identity verification on the user may be determined according to the credibility of the to-be-verified device and a correspondence between an identity verification policy and a credibility interval. A risk level matching the identity verification policy is in a negative relationship with a credibility of a user-held device.

[0100] During specific implementation, before step S105 is performed, the correspondence between an identity verification policy and a credibility interval may be preset. A higher device credibility indicates a more credible and reasonable device and a lower risk of allowing the device to log into or access a service system. Therefore, an identity verification policy matching the lower risk level may be adopted for performing identity verification. On the contrary, a lower device credibility indicates a less credible and less reasonable device and a higher risk of allowing the device to log into or access a service system. Therefore, an identity verification policy matching the higher risk level needs to be adopted for performing identity verification.

[0101] During determining, according to the credibility of the to-be-verified device, the

identity verification policy for performing identity verification on the user, when the credibility of the to-be-verified device falls within a specific credibility interval, an identity verification policy corresponding to the credibility interval may be determined as the identity verification policy for performing identity verification on the user by using the to-be-verified device.

[0102] It should be noted that one or more of: identity verification information, an identity verification information amount, and an identity verification threshold range may vary in different identity verification policies.

[0103] For example, when the identity verification policy includes an identity verification information type, a higher security level of the identity verification information type in the identity verification policy is more applicable to a lower credibility of the user-held device. Therefore, it may be understood that the security level of the identity verification information type is in a negative relationship with the credibility of the device. The security level of the identity verification information type may be defined according to a plurality of criteria. For example, because biological characteristics such as a fingerprint, a face, irises, and a voiceprint of a user are unique and irreproducible, it may be considered that identity verification information comprising the unique biological characteristic information of the user usually has a higher security level than identity verification information such as those in text message verification, password verification, security question verification, etc. For another example, it may be considered that a single-time valid dynamic short text message verification code has a higher security level than identity verification information such as those in a fixed security question. It may be understood that when the credibility of the user-held device is relatively low, identity verification information with a higher security level may be used for performing identity verification to ensure reliability of an identity verification result and security of the service system. When the credibility of the user-held device is relatively high, identity verification information with a lower security level may be used for performing identity verification to satisfy identity verification requirements of the identity verification system.

[0104] For another example, when the identity verification policy includes an identity verification information amount, a larger identity verification information amount in the identity verification policy is more applicable to a lower credibility of the user-held device. Therefore, it may be understood that the identity verification information amount is in a negative relationship with the credibility of the device. It may be understood that a larger identity verification information amount may indicate identity verification performed on the

user from more perspectives and bring a more reliable identity verification result. Optionally, when the user-held device has a relatively low credibility, the identity verification information amount may be increased to perform more comprehensive identity verification on the user and ensure the security of the service system. Optionally, when the user-held device has a relatively high credibility, the identity verification information amount may be reduced (for example, a security verification question number may be reduced) to simplify an identity verification process, improve identity verification efficiency, and increase user experience.

[0105] For another example, when the identity verification policy includes an identity verification threshold range, a larger identity verification threshold range in the identity verification policy is more applicable to a higher credibility of the user-held device. Therefore, it may be understood that the identity verification threshold range is in a positive relationship with the credibility of the device. Optionally, when the user-held device has a relatively low credibility, more strict identity verification needs to be performed on the user. Therefore, a relatively small identity verification threshold range may be adopted, and identity verification of a user without information falling within the range fails. When the user-held device has a relatively high credibility, more moderate identity verification may be performed on the user. Therefore, a relatively large identity verification threshold range may be adopted, and identity verification information of the user is more likely to fall within the range, facilitating identity verification success of the user and improving user experience.

[0106] In a scenario, it is assumed that the identity verification system uses face recognition information as the identity verification information. When the user-held device has a relatively high reliability, a face comparison threshold may be appropriately reduced, that is, a requirement on a degree of matching between face information of the user on which identity verification is performed and face information reserved in the identity verification system may be reduced, facilitating identity verification success of the user in a poor face collection environment such as insufficient light or uneven illumination for performing normal service processing.

[0107] Optionally, after the identity verification policy for performing identity verification on the user is determined, during identity verification 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 may be determined according to the identity verification policy. Then the identity verification system prompts, according to the identity verification process, the to-be-verified

device to report the information required for the identity verification. After receiving the prompt from the identity verification system, the to-be-verified device held by the user reports, according to the prompt, the information required for the identity verification. For example, when the information required for the identity verification is received from the to-be-verified device, the identity verification is performed according to the identity verification threshold range of the information required for the identity verification.

[0108] The main implementation process of this embodiment of the present application is described above by using examples. It may be understood that, in this embodiment of the present application, after the verification request is received from the to-be-verified device, the verification is not directly performed, but the credibility of the to-be-verified device is determined according to the device environment information of the historical device and the device environment information of the to-be-verified device, and the identity verification policy for performing identity verification on the user is further determined according to the credibility. According to the method in the embodiments of the present application, without awareness of a user, an identity verification policy applicable to a current user-held device can be selected for the user according to a credibility of the user-held device. Therefore, the embodiments of the present application facilitate improvements in the security and the reliability of identity verification, and can satisfy usage requirements of the user, and improve the user experience.

[0109] An optional manner of performing step S103 of determining the credibility of the to-be-verified device according to the historical feature information and the device environment information is further described below by using examples. For example, referring to FIG. 2, the following steps may be performed.

[0110] S1031: Determine a feature vector corresponding to the to-be-verified device according to the device environment information when a type of information included in the device environment information matches a preset information type.

[0111] It may be understood that the identity verification system may preset, according to different device types, preset information types for determining the credibility. Optionally, the preset information type may include an identity ID of a device, an IP address on a network to which the device is connected, Wi-Fi, and an LBS. For devices normally connected to a network, complete device environment information needs to include information of all preset information types. If the device environment information received by the identity verification system is missing (in this case, the type of the information included in the device environment information does not match the preset information type),

and the identity verification system cannot determine whether the cause is from an objective network environment, or subjective and intentional obstruction or evasion performed by an illegal user, the identity verification system may directly determine that the to-be-verified device is incredible, that is, the credibility of the to-be-verified device is at the lowest level.

[0112] When the type of the information included in the device environment information matches the preset information type, the identity verification system may determine the received device environment information as valid information. Therefore, the feature vector corresponding to the to-be-verified device may be determined according to the device environment information on this basis.

[0113] The feature vector may be determined according to the device environment information in a plurality of manners. Optionally, the feature vector may be determined according to the device environment information of the to-be-verified device and the historical feature information.

[0114] For example, it may be determined whether the device environment information of the to-be-verified device is consistent with the device environment information of the historical device, and a determining result is used as one or more components of the feature vector. When there are a plurality of specific contents in the device environment information, each specific content may be compared separately. The comparison process may be understood as determining whether the device environment information of the historical device includes the device environment information of the to-be-verified device, which is equivalent to determining whether the to-be-verified device has participated in the service system or whether the network environment to which the to-be-verified device is connected has been accessed by users with other devices. It should be noted that comparison results of all of the contents may be used as different sub-items in the feature vector, or the comparison results may be summarized by using a preset rule to be collectively used as the sub-items in the feature vector. For example, the preset rule may be that when the comparison results of the plurality of contents are all consistent, a value of the component in the feature vector is 1, and when a comparison result of any of the plurality of contents is inconsistent, the value of the component in the feature vector is 0.

[0115] For another example, it may be determined whether the device environment information of the to-be-verified device is consistent with device environment information with maximum historical connecting times, and a determining result is used as one or more components of the feature vector. For still another example, the device environment information of the to-be-verified device may be compared to a missing value of the device

environment information of the historical device, and one or more components in the feature vector may be determined according to the comparison result. Specific comparison and determining processes and a manner of determining the corresponding component in the feature vector according to the determining result obtained through comparison are similar to those in the foregoing examples, and details are not described herein again.

[0116] It may be understood that during determining of the feature vector corresponding to the to-be-verified device, device environment information existing when the user uses the to-be-verified device and device environment information of a device historically used by the user are used for comparison. In many normal cases, the device environment information of the user usually does not change. If the user-held device is unchanged (in this case, the identity ID of the device is unchanged), and network environment information (for example, an LBS) is changed, it may be still possible that the user sends a normal verification request. However, there is still a risk that the device is stolen. However, if the user-held device is changed (in this case, the identity ID of the device is changed), and the network environment information is unchanged, it is very likely that the user initiates the identity verification request with a changed device. If the device environment information (including identification information of the device and the network environment information) corresponding to the user does not match the historical feature information, allowing the to-be-verified device to access the service system brings a greater risk. Therefore, a more strict identity verification policy matching a higher risk may be adopted for performing identity verification on the user.

[0117] S1033: Input the feature vector to a device verification model, and determine the credibility of the to-be-verified device by using the device verification model. 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.

[0118] After the corresponding feature vector is generated according to the device environment information of the to-be-verified device, the device verification model may be further used to determine the credibility of the to-be-verified device. It may be understood that the credibility of the device may be embodied in a credibility label of the device output by the device verification model and the probability that the identity verification request sent by the device is predicted as a credible request. It should be noted that, determining of the identity verification policy according to the credibility of the to-be-verified device may be embodied as follows: determining a credibility interval within which the credibility label

and/or the probability that the identity verification request is predicted as a credible request falls according to the credibility label of the device and the probability that the identity verification request sent by the device is predicted as a credible request, and further determining an identity verification policy corresponding to the credibility interval as the identity verification policy for the user applying for identity verification with the held to-be-verified device.

[0119] Optionally, the device verification model may be established and trained offline by using a machine learning algorithm. For example, referring to FIG. 3, before the feature vector is input to the device verification model and the credibility of the to-be-verified is determined by using the device verification model, the following steps may be performed to complete the training and verification of the device verification model.

[0120] S201: Obtain historical feature information corresponding to the historical device.

[0121] Referring to FIG. 4, it may be understood that the historical feature information obtained by performing step S201 may be offline historical feature information corresponding to the historical device. The historical device may be either a historical login device logged into the service system (historical login information in historical feature information generated by the historical login device) or a historical identity verification device that undergoes identity verification (including successful identity verification and unsuccessful identity verification) and that performs service processing in the service system (historical identity verification information in historical feature information generated by the historical identity verification device).

[0122] It should be noted that during training of the device verification model, device verification models suitable for different users may be trained according to different contents of the historical feature information. For a user using the service system for the first time, since the user merely logs into the system, the historical feature information may include only device environment information of a historical login device (which may be referred to as historical login information in short) without device environment information of a historical identity verification device. Therefore, for a device verification model suitable for such users, an input parameter of the device verification model is determined with reference to only the historical login information in the historical feature information. For a user who underwent identity verification, since the user performed an identity verification operation, or even performed a service operation in the service system, the historical feature information may include both historical login information and historical identity verification information. Therefore, for a device verification model suitable for such users, an input parameter of the

device verification model may be determined with reference to both the historical login information and the historical core body information.

[0123] S203: Determine, 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.

[0124] Optionally, according to the time interval corresponding to the historical feature information, first historical feature information generated at an earlier moment may be assigned to the training set, and second historical feature information generated at a later moment may be assigned to the verification set. Since the historical feature information in the verification set is generated at a later moment, the historical feature information more satisfies current application requirements of the user. Therefore, assigning the historical feature information generated at a later moment to the verification set enables a more accurate determination of whether a verification result output by the device verification model is correct. For example, referring to FIG. 4, historical feature information generated at identity verification/login moments in recent 50 days may be extracted for training the device verification model. Historical feature information generated in recent 10 days is used as the second historical feature information to form the verification set, and the remaining historical feature information generated in recent 40 days is used as the first historical feature information to form the training set.

[0125] Optionally, the historical feature information includes network environment information such as an ID, Wi-Fi, an LBS, and IP of the device used by the user for login/identity verification. The historical feature information may further reflect an application scenario corresponding to the identity verification request initiated by the user, for example, logging into the service system, secondary verification of online payment, or modification of a payment password, etc. The historical feature information may further reflect a corresponding identity verification information type in the identity verification policy determined according to the credibility of the device, for example, face verification, fingerprint verification, or text message verification code verification, etc. The historical feature information may further reflect a verification result corresponding to a login/identity verification event.

[0126] S205: Train the device verification model by using the first historical feature information.

[0127] Optionally, the established device verification model may include a logistic regression (LR) model and an extreme gradient boosting XGBoost model. The training of the

device verification model by using the first historical feature information generally includes two parts: first-stage LR model training and second-stage XGBoost model training. An input of the XGBoost model includes an output of the LR model. Referring to FIG. 4, the entire training process of the device verification model is performed in series.

[0128] For example, referring to FIG. 4 and FIG. 5, the training of the device verification model may include the following steps.

[0129] S2051: Determine, 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.

[0130] Optionally, the credibility label of the device corresponding to the historical feature information may be, for example, a black sample and a white sample. It may be determined according to a status of a historical case, whether a historical identity identification request is allowed or refused, or an illegal operation on the service system when identity verification succeeds, etc. whether the credibility label is a black sample or a white sample.

[0131] For example, according to the status of the historical case, if a device is involved in a plurality of cases or a case with a relatively large amount of money, a credibility label of the device may be marked as a black sample. An identity verification request corresponding to historical feature information corresponding to the device may also be marked as an incredible request. The case herein may mean that an illegal user uses the device to enter an account of a legal user and illegally obtains money in the account of the legal user, etc.

[0132] For another example, if a historical identity verification request sent by a historical device is refused a plurality of times, it indicates that the device is likely to be illegally used. In this case, a credibility label of the device may be marked as a black sample, and an identity verification request corresponding to historical feature information corresponding to the device may also be marked as an incredible request.

[0133] For another example, if identity verification succeeds but a user performs an illegal service operation on the service system by using a device, a credibility label of the device may be marked as a black sample. An identity verification request corresponding to historical feature information corresponding to the device may also be marked as an incredible request.

[0134] It may be understood that the definition of and a method for determining a credibility label of a device is not limited to the above examples. According to specific application requirements, different meanings may be given to a credibility label, and the credibility label may be determined by using different methods. No limitation is imposed on this in this embodiment of the present application.

[0135] Optionally, for determining the feature vector based on the historical feature information, during training of the device verification model, offline statistics may be performed by using offline historical feature information to obtain the feature vector. Specifically, accumulative calculation of feature vectors may be performed according to different time windows and different user principals (which may be distinguished by using user identifiers). Optionally, historical behaviors may be accumulated in different perspectives such as a time window, a device identifier, a user identity, and a combination thereof, and a corresponding component in the feature vector may be determined according to an accumulated value. Alternatively, for each piece of historical feature information, it is determined whether current device environment information is consistent with environment information for a historical device, whether the current device environment information is consistent with the device environment information with maximum times of historical successful logins and/or successful identity verification, and the corresponding component in the feature vector is determined according to a determining result. The corresponding component in the feature vector may also be determined according to a number of factors, such as a comparison result of missing values of the current device environment information and the historical environment information, and a change in the device environment information in a preset number of recent days, etc.

[0136] Optionally, for determining the feature vector based on the historical feature information, during a usage phase of the device verification model, online real-time statistics may be determined by using real-time device environment information to obtain the feature vector, so as to monitor the output of the device verification model in real time and evaluate the device verification model. When evaluation data of the device verification model does not meet a preset condition, the device verification model may be updated, that is, updated historical feature information is used as the training set and the verification set to retrain the device verification model.

[0137] It should be noted that a number of components in the feature vector may be determined according to actual requirements of the identity verification system and the service system. Optionally, a number of components in the first historical feature vector input to the logistic regression LR model may be greater than a number of components in the second historical feature vector input to the extreme gradient boosting XGBoost model. For example, the first historical feature vector extracted from the historical feature information may have about 300 components, which are input to the logistic regression LR model. For the second historical feature vector extracted from the historical feature information, weights of

components in the feature vector may be considered, and features that can be used to distinguish between black and white samples may be further determined based on historical experience, so that more than 30 components may be selected from more than 300 components as the components of the second historical feature vector.

[0138] It should be further noted that for a device verification model applicable to a user using the service system for the first time, historical feature information used during training includes only device environment information of a historical login device (which may be referred to as historical login information in short) without device environment information of a historical identity verification device (which may be referred to as historical identity verification information for short). Correspondingly, the feature vector input into the model also includes only a component reflecting the historical login information without a component reflecting the historical identity verification information.

[0139] For a device verification model applicable to a user who underwent identity verification, historical feature information used during training includes both the historical login information and the historical identity verification information. Therefore, the feature vector input to the model includes both a component reflecting the historical login information and a component reflecting the historical identity verification information.

[0140] S2053: Input the first historical feature vector to the logistic regression LR model, and adjust a model parameter of the logistic regression LR model according to the first credibility label and a first target label output by the logistic regression LR model until the output of the logistic regression LR model satisfies a preset condition.

[0141] Optionally, during training of the logistic regression LR model, one or more of model parameters such as a regularization term, a regularization coefficient, and a maximum iteration number may be adjusted until the output of the logistic regression LR model satisfies the preset condition.

[0142] It may be understood that the first historical feature vector is input to the LR model, and the LR model outputs the first target label. The first target label is a credibility label of the device corresponding to the historical feature information in the generated first historical feature vector predicted by the logistic regression LR model. Based on the calibrated first credibility label, it may be determined whether the first target label output by the logistic regression LR model is correct and accurate, and then the model parameter of the logistic regression LR model is adjusted according to a determining result, so that the logistic regression LR model can output a sufficiently accurate target label. In addition, an optimal logistic regression LR model is obtained by adjusting a model parameter such as a

regularization term, a maximum iteration number, and a regularization coefficient, etc.

[0143] S2055: Calculate, according to an output of the trained logistic regression 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.

[0144] After the training of the logistic regression LR model is completed, a probability that the identity verification request is predicted as a white sample (that is, the first probability) may be calculated according to the output of the logistic regression LR model, which is used as one of input parameters of the extreme gradient boosting XGBoost model for training the extreme gradient boosting XGBoost model, which is shown in FIG. 4.

[0145] S2057: Input the first probability and the second historical feature vector to the extreme gradient boosting XGBoost model; and adjust a model parameter of the extreme gradient boosting XGBoost model by using an output of the extreme gradient boosting XGBoost model and the first credibility label until the output of the extreme gradient boosting XGBoost model satisfies a preset condition. The output of the extreme gradient boosting XGBoost model includes the 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.

[0146] Optionally, parameter adjustment of the extreme gradient boosting XGBoost mainly involves the adjustment of parameters such as a number of trees and a step size, etc.

[0147] It may be understood that the first probability calculated according to the output of the logistic regression LR model is used as one of the input parameters of the extreme gradient boosting XGBoost model, and the second historical feature vector is used as remaining input parameters of the extreme gradient boosting XGBoost model to obtain an output of the extreme gradient boosting XGBoost model, that is, the 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. The credibility label output by the extreme gradient boosting XGBoost model is compared to the calibrated first credibility label, so that it may be determined whether the credibility label output by the extreme gradient boosting XGBoost model is correct and accurate, and then the model parameter of the extreme gradient boosting XGBoost model is adjusted, so that the extreme gradient boosting XGBoost model can output a sufficiently correct credibility label. In addition, the number of trees and the step size are adjusted to obtain an optimal extreme gradient boosting XGBoost model.

[0148] S207: Verify the device verification model by using the second historical feature

information.

[0149] It may be understood that the verification of the device verification model may be performed immediately after the training of the device verification model is completed to determine whether accuracy of the output of the device verification model can meet application requirements. It should be noted that after the device verification model is used for a period of time, an output effect of the device verification model may be regularly or irregularly verified, so that when the output of the device verification model is not sufficiently accurate and cannot meet the application requirements, the device verification model is retrained by using updated historical feature information to meet the application requirements.

[0150] Optionally, referring to FIG. 6, during verification of the device verification model, the following methods may be used.

[0151] S2071: Determine, 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.

[0152] S2073: Input the third historical feature vector to the trained logistic regression LR model; and calculate, according to the output of the trained logistic regression 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.

[0153] S2075: Input the second probability and the fourth historical feature vector to a trained extreme gradient boosting XGBoost model, and obtaining an output of the device verification model by using the trained extreme gradient boosting XGBoost model. The output of the device verification model includes the 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.

[0154] S2077: Obtain 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.

[0155] S2079: Adjust the model parameter of the logistic regression LR model and/or the model parameter of the extreme gradient boosting XGBoost model according to the evaluation data until the evaluation data of the device verification model satisfies a preset condition.

[0156] It may be understood that the second historical feature information in the verification set is used as the input of the device verification model. After processing

performed by the logistic regression LR model and the extreme gradient boosting XGBoost model in series in the device verification model, the credibility label of the historical device corresponding to the second historical feature information and the third probability that the identity verification request sent by the historical device is predicted as a credible request are output. Then the evaluation data of the device verification model may be obtained by using a binary classification method according to the calibrated second credibility label.

[0157] Optionally, the evaluation data of the device verification model may include at least one of an F1 score and an area under the curve (AUC) value. For example, the F1 score is a parameter index giving comprehensive consideration to model precision and recall. A higher F1 score indicates a more robust classification model (which is specifically the device verification model herein). The area under the curve AUC value is a possibility that a probability that a given positive sample output by the classification module is positive is greater than a probability that a negative sample output by the classification model is positive. The F1 score and the area under the curve AUC value are used for judging training of a model. An effect of predicting the credibility by the model is evaluated by using the evaluation data of the model, and the model parameter of the logistic regression LR model and/or the model parameter of the extreme gradient boosting XGBoost model are/is continuously adjusted, so as to obtain an optimal model combination of the logistic regression LR model and the extreme gradient boosting XGBoost model.

[0158] It should be noted that in actual application, for the evaluation data of the device verification model, in addition to mathematical parameters of the model, a misjudgment rate of black samples and an accuracy rate of white samples may be further considered with reference to the actual application scenario of the model. If a black sample is determined as a white sample, identity verification of an illegal user succeeds, threatening the security of the service system. If a white sample is determined as a black sample, although the security of the service systems is not affected due to strict identity verification on a legal user, the user experience is affected. Therefore, judgement accuracy and a misjudgment rate of the device verification model also need to be considered. When the accuracy rate decreases and misjudgment rate increases, model update may be triggered, that is, the device verification model is retrained by using the updated historical feature information.

[0159] In the embodiments of the present application, after the verification request is received from the to-be-verified device, the verification is not directly performed, but the credibility of the to-be-verified device is determined according to the device environment information of the historical device and the device environment information of the

to-be-verified device, and the identity verification policy for performing identity verification on the user is further determined according to the credibility. According to the method in the embodiments of the present application, without awareness of a user, an identity verification policy applicable to a current user-held device can be selected for the user according to a credibility of the user-held device. Therefore, the embodiments of the present application facilitate improvements in the security and the reliability of identity verification, and can satisfy usage requirements of the user, and improve the user experience.

[0160] An embodiment of the present application further provides an identity verification apparatus applied to an identity verification system. Referring to FIG. 7, the identity verification apparatus may include:

[0161] a request receiving module 101 configured to receive an identity verification request from a to-be-verified device, where the identity verification request includes 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;

[0162] a credibility determining module 103 configured to determine a credibility of the to-be-verified device according to historical feature information and the device environment information, where the historical feature information includes device environment information of a historical device; and

[0163] an identity verification policy determining module 105 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.

[0164] It may be understood that the identity verification apparatus illustrated in FIG. 7 corresponds to the identity verification method performed by the identity verification system provided in the foregoing embodiment, and can implement the identity verification method in the foregoing embodiment. Details are not described herein again.

[0165] FIG. 8 is a structural schematic diagram of an electronic device according to an embodiment of the present application. Referring to FIG. 8, on a hardware level, the electronic device includes a processor, and optionally includes an internal bus, a network interface, and a memory, where the memory may include an internal memory, such as a random-access memory (RAM), or may further include a non-volatile memory, such as at least one magnetic-disk memory. Certainly, the electronic device may further include other hardware required by services.

[0166] The processor, the network interface, and the memory may be mutually connected

through an internal bus, and the internal bus may be an industry standard architecture (ISA) bus, a peripheral component interconnect (PCI) bus, or an extended industry standard architecture (EISA) bus. The bus may be divided into an address bus, a data bus, and a control bus. For ease of representation, only one thick line is used to represent the bus in FIG. 8, but this does not mean that there is only one bus or only one type of bus.

[0167] The memory is configured to store a program. For example, the program may include program code, the program code include computer executable instructions. The memory may include an internal memory and a non-volatile memory, and provide instructions and data for the processor.

[0168] The processor reads a corresponding computer program from the non-volatile storage into the internal memory and then runs the computer program, to form an identity verification apparatus. The processor executes the program stored in the memory, and the program is used for performing the following operations:

[0169] receiving an identity verification request from a to-be-verified device, where the identity verification request includes 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;

[0170] determining a credibility of the to-be-verified device according to historical feature information and the device environment information, where the historical feature information includes device environment information of a historical device; and

[0171] 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.

[0172] The foregoing method performed by the identity verification apparatus disclosed in the embodiment shown in FIG. 1 of the present application may be applied to a processor, or may be implemented by a processor. The processor may be an integrated circuit chip and has a signal processing capability. In an implementation process, steps of the foregoing method may be implemented by using a hardware integrated logic circuit in the processor or instructions in a form of software. The processor may be a general processor, including a central processing unit (Central Processing Unit, CPU), a network processor (Network Processor, NP), and the like; or may further be a digital signal processor (Digital Signal Processing, DSP), an application-specific integrated circuit (Application-Specific Integrated Circuit, ASIC), a field programmable gate array (Field-Programmable Gate Array, FPGA), or another programmable logical device, discrete gate or transistor logical device, or discrete

hardware component. The processor may implement or perform the methods, the steps, and logical block diagrams that are disclosed in the embodiments of the present application. The general-purpose processor may be a microprocessor, or the processor may further be any conventional processor, or the like. Steps of the methods disclosed with reference to the embodiments of the present application may be directly performed and completed by using a hardware decoding processor, or may be performed and completed by using a combination of hardware and software modules in the decoding processor. The software module may be located in a mature storage medium in the field, such as a random-access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically-erasable programmable memory, or a register. The storage medium is located in the memory, and the processor reads information in the memory and completes the steps in the foregoing methods in combination with hardware of the processor.

[0173] The electronic device may further perform the method performed by the identity verification apparatus in FIG. 1, and implement the function of the identity verification apparatus shown in the embodiment of FIG. 1. This is not repeated herein in the embodiment of the present application.

[0174] An embodiment of the present application further provides a computer readable storage medium. The computer readable storage medium stores one or more programs, the one or more programs include an instruction, and when the instruction is executed by an electronic device including a plurality of applications, the electronic device is enabled to perform the method performed by the identity verification apparatus in the embodiment shown in FIG. 1, and is specifically configured to perform the following steps:

[0175] receiving an identity verification request from a to-be-verified device, where the identity verification request includes 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;

[0176] determining a credibility of the to-be-verified device according to historical feature information and the device environment information, where the historical feature information includes device environment information of a historical device; and

[0177] 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.

[0178] A person skilled in the art should understand that the embodiments of the present application may be provided as a method, a system, or a computer program product.

Therefore, the present application may use a form of hardware only embodiments, software only embodiments, or embodiments with a combination of software and hardware. Moreover, the present application may use a form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, and the like) that include computer-usable program code.

[0179] The present invention is described with reference to the flowcharts and/or block diagrams of the method, the device (system), and the computer program product according to the embodiments of the present application. It should be understood that computer program instructions may be used to implement each process and/or each block in the flowcharts and/or the block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions may be provided for a general-purpose computer, a dedicated computer, an embedded processor, or a processor of any other programmable data processing device to generate a machine, so that the instructions executed by a computer or a processor of any other programmable data processing device generate an apparatus for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0180] These computer program instructions may also be stored in a computer readable memory that can guide a computer or another programmable data processing device to work in a specific manner, so that the instructions stored in the computer readable memory generate a product including an instruction apparatus, where the instruction apparatus implements functions specified in one or more procedures in the flowcharts and/or one or more blocks in the block diagrams.

[0181] These computer program instructions may also be loaded into a computer or another programmable data processing device, so that a series of operation steps are performed on the computer or another programmable data processing device to generate processing implemented by a computer, and instructions executed on the computer or another programmable data processing device provide steps for implementing functions specified in one or more procedures in the flowcharts and/or one or more blocks in the block diagrams.

[0182] In a typical configuration, the computer device includes one or more processors (CPU), an input/output interface, a network interface, and an internal memory.

[0183] The internal memory may include a form such as a volatile memory, a random access memory (RAM), and/or a non-volatile memory in a computer readable medium, for example, a read-only memory (ROM) or a flash memory (flash RAM). The internal memory is an example of the computer readable medium.

[0184] The computer-readable medium includes persistent, non-persistent, movable, and unmovable media that may implement information storage by using any method or technology. The information may be a computer readable instruction, a data structure, a program module or other data. An example of a computer storage medium includes, but is not limited to, a phase-change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of RAM, a ROM, an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a CD-ROM, a digital versatile disc (DVD) or another optical memory, a cassette, a magnetic tape, a magnetic disk memory or another magnetic storage device, or any other non-transmission medium, and may be used to store information accessible by the computing device. Based on the definition in the present disclosure, the computer-readable medium does not include transitory computer readable media (transitory media), such as a modulated data signal and a carrier.

[0185] It should also be noted that the terms “include,” “comprise,” and any other variants mean to cover the non-exclusive inclusion. Thereby, the process, method, article, or device which include a series of elements not only include those elements, but also include other elements which are not clearly listed, or include the inherent elements of the process, method, article and device. Unless otherwise specified, an element limited by “include a/an...” does not exclude other same elements existing in the process, the method, the article, or the device that includes the element.

[0186] A person skilled in the art should understand that the embodiments of the present application may be provided as a method, a system, or a computer program product. Therefore, the present application may use a form of total hardware embodiments, total software embodiments, or embodiments combining software and hardware. In addition, the present application may use a form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, and the like) that include computer-usable program code.

[0187] The foregoing descriptions are merely embodiments of the present application and are not intended to limit the present application. For a person skilled in the art, various modifications and variations can be made to the present application. Any modification, equivalent replacement, improvement and the like made within the spirit and principle of the present application should fall within the protection scope of the present application.

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;

obtaining historical feature information and the device environment information, wherein the historical feature information comprises device environment information of a historical device;

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

inputting the historical feature vector to a device verification model, wherein the device verification model comprises an XGBoost (extreme gradient boosting) model;

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 historical feature information and a probability that an identity verification request sent by the historical device is predicted as a credible request;

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;

outputting, from the device verification model based on the feature vector corresponding to the to-be-verified device, a credibility of the computing device; 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, the method further comprises:

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

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 the first historical feature information and a verification set comprising the second historical feature information comprises:

according to the time interval corresponding to the historical feature information, assigning the first historical feature information generated at an earlier moment to the training set, and assigning the 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 further comprises an LR (logistic regression) 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 the first credibility label of the 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;

generating the output of the XGBoost model based on inputting the first probability and the second historical feature vector to the XGBoost model.

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:

obtain historical feature information and the device environment information, wherein the historical feature information comprises device environment information of a historical device;

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

input the historical feature vector to a device verification model, wherein the device verification model comprises an XGBoost (extreme gradient boosting) model;

adjust 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 historical feature information and a probability that an identity verification request sent by the historical device is predicted as a credible request;

determine 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;

input the feature vector to the device verification model, and
output, from the device verification model based on the feature vector
corresponding to the to-be-verified device, a credibility of the computing device; 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;
obtaining historical feature information and the device environment information,
wherein the historical feature information comprises device environment information of a
historical device;
determine, according to the historical feature information, a historical feature vector and
a first credibility label of a historical device corresponding to the historical feature
information;
input the historical feature vector to a device verification model, wherein the device
verification model comprises an XGBoost (extreme gradient boosting) model;
adjust 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 historical feature information and a probability that
an identity verification request sent by the historical device is predicted as a credible request;
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 the device verification model;
outputting, from the device verification model based on the feature vector

corresponding to the to-be-verified device, a credibility of the computing device; 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;

obtaining historical feature information and the device environment information, wherein the historical feature information comprises device environment information of a historical device;

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

input the historical feature vector to a device verification model, wherein the device verification model comprises an XGBoost (extreme gradient boosting) model;

adjust 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 historical feature information and a probability that an identity verification request sent by the historical device is predicted as a credible request;

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 the device verification model;

outputting, from the device verification model based on the feature vector corresponding to the to-be-verified device, a credibility of the computing device; 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.