

## VERIFICATION METHOD AND DEVICE

[0001] The present application claims priority to Chinese Patent Application No. 201510946529.7, filed on December 16, 2015 and entitled "VERIFICATION METHOD AND DEVICE", which is incorporated herein by reference in its entirety.

5

### TECHNICAL FIELD

[0002] The present disclosure relates to the field of Internet technologies, and in particular, to a verification method and device.

### BACKGROUND

[0003] Currently, to protect properties of a user against damage, when the user performs a sensitive operation that is related to property security of the user, such as changing an account password, online shopping, or online transfer, a server will verify the user's identity to ensure that the operation is performed by the user. As such, the user can successfully achieve the purpose of changing the account password, online shopping, online transfer, etc. Among them, the commonly used verification method is short message service message-based verification.

[0004] Sometimes, a user may perform multiple sensitive operations related to property security of the user in a short period of time. Because a server verifies a user's identity via short message service message-based verification, each time the user performs a sensitive operation, the server will verify the user's identity multiple times via short message service message-based verification in the entire process. For example, the user first changes an account password, and immediately performs network payment after the changes were completed. When the user changes the account password, the server verifies the user's identity via short message service message-based verification. When the user performs network payment, the server will verify the user's identity again via short message service message-based verification.

## SUMMARY

[0005] To resolve the problem in the existing technology, the present disclosure provides a verification method and device.

[0006] A first aspect of the embodiments of the present disclosure provides a verification method, where the method includes: when verification needs to be performed on a user, obtaining a current local time; obtaining a verification method in which the user failed to gain verification in predetermined duration prior to the current time; and performing verification on the user by using the verification method in which the user failed to gain verification.

[0007] The obtaining a verification method in which the user failed to gain verification in predetermined duration prior to the current time includes: obtaining a verification method list, where each row in the verification method list includes at least one verification method; removing, from the verification method list, a verification method in which the user is verified in the predetermined duration prior to the current time; and obtaining a verification method in one row in a post-removal verification method list.

[0008] The removing, from the verification method list, a verification method in which the user is verified in the predetermined duration prior to the current time includes: obtaining a locally stored correspondence between a verification method and a passing time; searching the correspondence for a verification method corresponding to a passing time, where a difference between the passing time and the current time is smaller than the predetermined duration; and deleting the identified verification method from the verification method list.

[0009] The method further includes: when the user is verified in the verification method in which the user is previously unverified, obtaining a current local time and determining the current local time as a passing time when the user is verified in the verification method in which the user is previously unverified; and substituting, in the correspondence, the determined passing time for a passing time corresponding to the verification method in which the user is previously unverified.

[0010] After the removing, from the verification method list, a verification method in which the user is verified in the predetermined duration prior to the current time, the method further includes: determining whether the number of rows in the post-removal verification method list is smaller than the number of rows in the

pre-removal verification method list; and when the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list, determining that the user is currently verified; or when the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, performing the step of obtaining a verification method in one row in a post-removal verification method list.

**[0011]** A second aspect of the embodiments of the present disclosure provides a verification method, where the method includes: when verification needs to be performed on a user, obtaining a current local time; obtaining a verification method that has not been used to perform verification on the user in predetermined duration prior to the current time; and performing verification on the user by using the unused verification method.

**[0012]** The obtaining a verification method that has not been used to perform verification on the user in predetermined duration prior to the current time includes: obtaining a verification method list, where each row in the verification method list includes at least one verification method; removing, from the verification method list, a verification method that has been used to perform verification on the user in the predetermined duration prior to the current time; and obtaining a verification method in one row in a post-removal verification method list.

**[0013]** The removing, from the verification method list, a verification method that has been used to perform verification on the user in the predetermined duration prior to the current time includes: obtaining a locally stored correspondence between a verification method and a verification time; searching the correspondence for a verification method corresponding to a verification time, where a difference between the verification time and the current time is smaller than the predetermined duration; and deleting the identified verification method from the verification method list.

**[0014]** The method further includes: when verification is performed on the user by using the unused verification method, obtaining a current local time and determining the current local time as a verification time of performing verification on the user by using the unused verification method; and substituting, in the correspondence, the determined verification time for a verification time corresponding to the unused verification method.

**[0015]** After the removing, from the verification method list, a verification method that has been used to perform verification on the user in the predetermined

duration prior to the current time, the method further includes: determining whether the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list; and when the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list, determining that the user is currently verified; or when the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, performing the step of obtaining a verification method in one row in a post-removal verification method list.

10 **[0016]** A third aspect of the embodiments of the present disclosure provides a verification device, where the device includes: a first current time acquisition module, configured to: when verification needs to be performed on a user, obtain a current local time; a first verification method acquisition module, configured to obtain a verification method in which the user failed to gain verification in predetermined duration prior to the current time; and a first verification module, configured to perform verification on the user by using the verification method in which the user failed to gain verification.

15 **[0017]** A fourth aspect of the embodiments of the present disclosure provides a verification device, where the device includes: a second current time acquisition module, configured to: when verification needs to be performed on a user, obtain a current local time; a second verification method acquisition module, configured to obtain a verification method that has not been used to perform verification on the user in predetermined duration prior to the current time; and a second verification module, configured to perform verification on the user by using the unused verification method.

20 **[0018]** The technical solutions provided in the embodiments of the present disclosure can include the following beneficial effects: In the existing technology, a server verifies a user's identity via short message service message-based verification each time the user performs a sensitive operation. If the user performs multiple sensitive operations in a short period of time, the server will verify the user's identity multiple times by using the same verification method in a short period of time, resulting in relative low user experience.

25 **[0019]** In the embodiments of the present disclosure, when verification needs to be performed on a user, a verification method in which the user failed to gain

verification in predetermined duration prior to a current time is obtained; or a verification method that has not been used to perform verification on the user in predetermined duration prior to a current time is obtained. Then verify the user by the obtained verification method, avoiding using the same verification method to verify  
5 the user multiple times in a short period of time, and improving user experience.

**[0020]** It should be understood that both the foregoing general descriptions and the following detailed descriptions are merely exemplary and explanatory, and cannot limit the present disclosure.

### **BRIEF DESCRIPTION OF DRAWINGS**

10 **[0021]** The accompanying drawings here are incorporated in the specification, become a part of the specification, show embodiments that are in accordance with the present disclosure, and are used with the specification to explain the principle of the present disclosure.

**[0022]** FIG. 1 is a flowchart illustrating a verification method according to an  
15 exemplary embodiment;

**[0023]** FIG. 2 is a flowchart illustrating a verification method according to an exemplary embodiment;

**[0024]** FIG. 3 is a flowchart illustrating a verification method according to an exemplary embodiment;

20 **[0025]** FIG. 4 is a flowchart illustrating a verification method according to an exemplary embodiment;

**[0026]** FIG. 5 is a flowchart illustrating a verification method according to an exemplary embodiment;

**[0027]** FIG. 6 is a flowchart illustrating a verification method according to an  
25 exemplary embodiment;

**[0028]** FIG. 7 is a block diagram illustrating a verification device according to an exemplary embodiment; and

**[0029]** FIG. 8 is a block diagram illustrating a verification device according to an exemplary embodiment.

## DESCRIPTION OF EMBODIMENTS

[0030] Exemplary embodiments are described in detail here, and examples of the exemplary embodiments are presented in the accompanying drawings. When the following description refers to the accompanying drawings, unless otherwise indicated, same numerals in different accompanying drawings represent the same or similar element. Implementations described in the following exemplary embodiments do not represent all implementations consistent with the present disclosure. On the contrary, they are only examples of apparatuses and methods consistent with some aspects of the present disclosure as detailed in the appended claims.

10 [0031] FIG. 1 is a flowchart illustrating a verification method according to an exemplary embodiment. As shown in FIG. 1, the method includes the following steps.

[0032] In step S101, a current local time is obtained when verification needs to be performed on a user.

15 [0033] In the process of using the terminal, the user sometimes needs to perform a sensitive operation that is related to property security of the user on the terminal, for example, changing an account password, online shopping, or online transfer. When the terminal receives a user's input that is a sensitive operation closely relating to property security of the user, it generates a sensitive request and sends the sensitive request to a server. When the server receives the sensitive request sent by the terminal, 20 to ensure property security of the user, the server needs to perform verification on the identity of the user before responding to the sensitive request, to ensure that the sensitive operation is performed by the user. When the user is verified, the server responds to the sensitive request.

25 [0034] For the server, when receiving the sensitive request sent by the terminal, it determines to perform verification on the user and obtains the current local time.

[0035] In step S102, a verification method in which the user failed to gain verification in predetermined duration prior to the current time is obtained.

[0036] The predetermined duration can be a duration that is set by a technician on the server in advance, and can be 30 seconds, 1 minute, or 2 minutes, and the like.

30 This is not limited in the present disclosure.

[0037] Among them, there are many verification methods for the server to verify the user. For example, short message service message-based verification, email-based verification, facial verification, security question verification, fingerprint verification,

etc.

**[0038]** For example, suppose the predetermined duration is 10 minutes. Within 10 minutes prior to the current time, if the server performs verification on the identity of the user via short message service message-based verification, and the user is verified, the short message service message-based verification is a verification method in which the user is verified in the predetermined duration prior to the current time. Within 10 minutes prior to the current time, if the server performs verification on the identity of the user via email-based verification, but the user failed to gain verification, the email-based verification is a verification method in which the user failed to gain verification in the predetermined duration prior to the current time.

**[0039]** In step S103, verification is performed on the user by using the verification method in which the user failed to gain verification.

**[0040]** In the existing technology, a server performs verification on an identity of a user via short message service message-based verification each time the user performs a sensitive operation. If the user performs multiple sensitive operations in a short period of time, the server performs verification on the user multiple times by using the same verification method in a short period of time, resulting in relatively low user experience

**[0041]** In this embodiment of the present disclosure, when verification needs to be performed on a user, a verification method in which the user failed to gain verification in predetermined duration prior to a current time is obtained, and then verification is performed on the user by using the obtained verification method. Therefore, using the same verification method to verify the user multiple times in a short period of time is avoided, and user experience is improved.

**[0042]** In another embodiment of the present disclosure, as shown in FIG. 2, step S102 includes the following steps.

**[0043]** In step S201, a verification method list is obtained.

**[0044]** There are multiple rows in the verification method list. Each row includes at least one verification method, and verification methods included in any two rows are not completely the same. If a row includes multiple verification methods, any two verification methods in the row are different.

**[0045]** For example, the verification method list can be shown in Table 1. There are three rows in Table 1. The first row includes two verification methods: short message service message-based verification and email-based verification. The second

row includes one verification method: facial verification. The third row includes two verification methods: email-based verification and security question verification.

**Table 1**

|                                                                               |
|-------------------------------------------------------------------------------|
| Short message service message-based verification and email-based verification |
| Facial verification                                                           |
| Email-based verification and security question verification                   |

5    **[0046]**    In step S202, a verification method in which the user is verified in the predetermined duration prior to the current time is removed from the verification method list.

**[0047]**    The present step can be specifically implemented in the following processes, including:

10   **[0048]**    (11) Obtain a locally stored correspondence between a verification method and a passing time.

**[0049]**    In this embodiment of the present disclosure, each time the server performs verification on the user by using a certain verification method. If the user passes the verification method, the server obtains a passing time indicating the time  
15   the user is verified by the verification method, and then searches the locally stored correspondence between a verification method and a passing time to determine whether the verification method exists.

**[0050]**    When the correspondence does not include the verification method, it indicates that the user is previously unverified by the verification method. In this case,  
20   the verification method and the passing time are stored as one record in the correspondence.

**[0051]**    When the correspondence includes the verification method, it indicates that the user is previously verified by the verification method. In this case, the correspondence needs to be searched for a passing time corresponding to the  
25   verification method, and then the obtained passing time is substituted for the identified passing time, so that the passing time indicating the time the user is verified by the verification method can be updated.

**[0052]**    As such, when a latest passing time when the user is previously verified by a certain verification method needs to be searched for, the server can obtain the

locally stored correspondence between a verification method and a passing time, and then search the correspondence for a passing time corresponding to the verification method, so as to obtain the latest passing time when the user is previously verified by the verification method.

- 5   **[0053]**     For example, the correspondence between a verification method and a passing time can be shown in Table 2.

**Table 2**

| Verification method                              | Passing time |
|--------------------------------------------------|--------------|
| Email-based verification                         | 09:09:22     |
| Short message service message-based verification | 13:05:27     |
| Facial verification                              | 12:08:12     |
| Security question verification                   | 11:32:45     |
| Fingerprint verification                         | 13:01:21     |

- 10   **[0054]**     As shown in Table 2, previously, verification methods by which the user is verified include email-based verification, short message service message-based verification, facial verification, security question verification, and fingerprint verification. The latest passing time when the user is verified via email-based verification is 09:09:22, the latest passing time when the user is verified via short message service message-based verification is 13:05:27, the latest passing time when the user is verified via facial verification is 12:08:12, the latest passing time when the user is verified via security question verification is 11:32:45, and the latest passing time when the user is verified via fingerprint verification is 13:01:21.

- 15   **[0055]**     (12) Search the correspondence for a verification method corresponding to a passing time, where a difference between the passing time and the current time is smaller than the predetermined duration.

- 20   **[0056]**     A passing time included in any record in the correspondence is obtained. The passing time is subtracted from the current time to obtain duration. The duration is compared with the predetermined duration. If the duration is smaller than the predetermined duration, a verification method included in the record is obtained and
- 25   is used as a verification method corresponding to a passing time, where a difference

between the passing time and the current time is smaller than the predetermined duration.

**[0057]** The described operation is performed on any other record in the correspondence. As such, all verification methods corresponding to passing times are identified from the correspondence, where a difference between the passing time and the current time is smaller than the predetermined duration.

**[0058]** For example, the current time is 13:10:04, and the predetermined duration is 10 minutes. Passing times 13:05:27 and 13:01:21 can be identified from the correspondence shown in Table 2, where a difference between the passing time and the current time 13:10:04 is smaller than 10 minutes, and it can be determined that verification methods corresponding to the two passing times are respectively short message service message-based verification and fingerprint verification.

**[0059]** (13) Delete the identified verification method from the verification method list.

**[0060]** Specifically, the verification method list is searched for any verification method identified in step (12). When the verification method list includes the verification method, the verification method is deleted from the verification method list. The described operation is performed for any other verification method identified in step (12). As such, all verification methods identified in step (12) are deleted from the verification method list.

**[0061]** For example, in the example in step (12), identified verification methods are short message service message-based verification and fingerprint verification. The verification method list shown in Table 1 is searched for short message service message-based verification, and it is determined that the verification method list shown in Table 1 includes short message service message-based verification. In this case, short message service message-based verification is deleted from the verification method list shown in Table 1, to obtain a verification method list shown in Table 3.

**Table 3**

|                                                             |
|-------------------------------------------------------------|
| Email-based verification                                    |
| Facial verification                                         |
| Email-based verification and security question verification |

[0062] Then the verification method list shown in Table 3 is searched for fingerprint verification, and it is determined that the verification method list shown in Table 3 does not include fingerprint verification. In this case, the verification method  
5 list shown in Table 3 is determined as a post-removal verification method list.

[0063] In step S203, a verification method in one row in a post-removal verification method list is obtained.

[0064] The purpose of the present disclosure is to determine one row from the verification method list and perform verification on the user by using all verification  
10 methods in the determined row. After the user is verified in all the verification methods in the determined row, the server can determine that the user is currently verified.

[0065] Therefore, in this embodiment of the present disclosure, the server can actively select one row from the post-removal verification method list. For example, the server can randomly select one row from the post-removal verification method  
15 list, and then obtain all verification methods in the selected row.

[0066] In another embodiment of the present disclosure, the server can send the post-removal verification method list to the terminal, so that the terminal displays the post-removal verification method list to the user. The user can select one row from the post-removal verification method list displayed by the terminal. The terminal sends  
20 the row selected by the user to the server. The server obtains a verification method in the row selected by the user.

[0067] The server can determine that the user is currently verified only after the user is verified in all verification methods in one row in the verification method list. Therefore, if the user selects a row that includes only one verification method, the user  
25 can be currently verified if the user is verified by that verification method. If the user selects a row that includes multiple verification methods, the user can be currently verified only if the user is verified by the multiple verification methods separately. Therefore, the user usually selects a row that includes fewer verification methods from the post-removal verification method list, so that the user can be  
30 currently verified as soon as possible.

[0068] For example, in the post-removal verification method list shown in Table 3, the first row and the second row include fewer verification methods, but the third row includes more verification methods. Therefore, the user usually selects the first row or the second row to be currently verified.

[0069] Therefore, in the present step, if the server actively selects one row from the post-removal verification method list, the server can select a row that includes fewer verification methods, so that the user can be currently verified as soon as possible.

5 [0070] As described in the previous embodiment, the user can be currently verified once the user is verified in all verification methods in any row in the verification method list. Therefore, to ensure the user be currently verified as soon as possible, in another embodiment of the present disclosure, after step S202, as shown in FIG. 3, the method further includes the following steps.

10 [0071] In step S301, it is determined whether the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list.

[0072] In some situations, if all verification methods in a certain row in the verification method list are verification methods in which the user is verified in the  
15 predetermined duration prior to the current time, all the verification methods in the row are removed in step S202, that is, the row is no longer included in the verification method list. As such, the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list.

[0073] For example, if verification methods in which the user is verified in the  
20 predetermined duration prior to the current time are short message service message-based verification and facial verification, short message service message-based verification and facial verification are removed from the verification method list shown in Table 1 in step S202, to obtain a verification method list shown in Table 4.

25 **Table 4**

|                                                             |
|-------------------------------------------------------------|
| Email-based verification                                    |
| Email-based verification and security question verification |

[0074] There are two rows in the verification method list shown in Table 4, but there are three rows in the pre-removal verification method list shown in Table 1. As such, it can be determined that the number of rows in the post-removal verification  
30 method list is smaller than the number of rows in the pre-removal verification method

list. Then step S302 is performed.

**[0075]** In step S302, when the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list, it is determined that the user is currently verified.

5 **[0076]** In this embodiment of the present disclosure, the user can be currently verified once the user is verified in all verification methods in any row in the verification method list. Therefore, once it is determined that the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list, it indicates that the user is verified in all  
10 verification methods in any one of removed rows in the predetermined duration prior to the current time. Therefore, no verification needs to be performed on the user, and it can be determined that the user is currently verified. The process ends.

**[0077]** When the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, step S203 is performed: Obtain a verification method in one row in a post-removal verification  
15 method list.

**[0078]** In this embodiment of the present disclosure, when the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, verification methods in one row may include  
20 verification methods in another row in the post-removal verification method list, that is, the row includes the verification methods in the another row, but the number of verification methods in the row is greater than the number of verification methods in the another row.

**[0079]** For example, in the verification method list shown in Table 3, verification  
25 methods in the third row are email-based verification and security question verification, and a verification method in the first row is email-based verification. The third row includes email-based verification in the first row, and the number of verification methods in the third row is greater than the number of verification methods in the first row. Therefore, the verification methods in the third row include  
30 the verification method in the first row.

**[0080]** The user can be currently verified once the user is verified via email-based verification if the user selects the first row, but the user can be currently verified only when the user is verified via both email-based verification and security question verification if the user selects the third row. Therefore, the user usually prefers the

first row to the third row to be currently verified as soon as possible.

[0081] However, the server may sometimes actively select one row from the post-removal verification method list. If the server selects the third row instead of the first row, the user needs to be verified via both email-based verification and security question verification. In this case, the user cannot be currently verified as soon as possible.

[0082] Therefore, in this embodiment of the present disclosure, when the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, the server determines whether verification methods in any row in the post-removal verification method list include verification methods in another row. When the verification methods in the row include verification methods in another row, the server deletes the row from the post-removal verification method list. The server performs the described operation on any other row.

[0083] For example, the third row is deleted from the verification method list shown in Table 3, to obtain a verification method list shown in Table 5. When selecting one row from the verification method list shown in Table 5, besides selecting the second row that includes facial verification, the server can select the first row that includes email-based verification, and the server cannot select the original third row that includes email-based verification and security question verification in Table 3. As such, the server performs verification on the user only via email-based verification, and the user can be currently verified once the user is verified via email-based verification. Therefore, the user can be verified as soon as possible, and verification efficiency is increased.

**Table 5**

|                          |
|--------------------------|
| Email-based verification |
| Facial verification      |

[0084] Further, in the described embodiment of the present disclosure, after the server performs verification on the user by using a verification method in which the user failed to gain verification, when the user is verified in the verification method, the server obtains a current local time and uses the current local time as a passing time when the user is verified in the verification method, and then substitutes, in the locally

stored correspondence between a verification method and a passing time, the passing time for a passing time corresponding to the verification method, so that the passing time indicating the time the user is verified by the verification method can be updated.

**[0085]** FIG. 4 is a flowchart illustrating a verification method according to an exemplary embodiment. As shown in FIG. 4, the method includes the following steps.

**[0086]** In step S401, a current local time is obtained when verification needs to be performed on a user.

**[0087]** In the process of using the terminal, the user sometimes needs to perform a sensitive operation that is related to property security of the user on the terminal, for example, changing an account password, online shopping, or online transfer. When the terminal receives a user's input that is a sensitive operation closely relating to property security of the user that is input by the user, it generates a sensitive request and sends the sensitive request to a server. When the server receives the sensitive request sent by the terminal, to ensure property security of the user, the server needs to perform verification on the identity of the user before responding to the sensitive request, to ensure that the sensitive operation is performed by the user. When the user is verified, the server responds to the sensitive request.

**[0088]** For the server, when receiving the sensitive request sent by the terminal, it determines to perform verification on the user and obtains the current local time.

**[0089]** In step S402, a verification method that has not been used to perform verification on the user in predetermined duration prior to the current time is obtained.

**[0090]** The predetermined duration can be a duration that is set by a technician on the server in advance, and can be 30 seconds, 1 minute, or 2 minutes, and the like. This is not limited in the present disclosure.

**[0091]** Among them, there are many verification methods for the server to verify the user. For example, short message service message-based verification, email-based verification, facial verification, security question verification, fingerprint verification, etc.

**[0092]** In this embodiment of the present disclosure, the server may perform verification on the user only by using some of the multiple verification methods in the predetermined duration prior to the current time.

**[0093]** For example, suppose the predetermined duration is 10 minutes. Within 10 minutes prior to the current time, if the server performs verification on the identity of the user via short message service message-based verification, the short message

service message-based verification is a verification method that has been used to perform verification on the user in the predetermined duration prior to the current time. With 10 minutes prior to the current time, if the server does not perform verification on the identity of the user via email-based verification, the email-based verification is a verification method that has not been used to perform verification on the user in the predetermined duration prior to the current time.

**[0094]** In step S403, verification is performed on the user by using the unused verification method.

**[0095]** In the existing technology, a server performs verification on an identity of a user via short message service message-based verification each time the user performs a sensitive operation. If the user performs multiple sensitive operations in a short period of time, the server performs verification on the user multiple times by using the same verification method in a short period of time, resulting in relatively low user experience

**[0096]** In this embodiment of the present disclosure, when verification needs to be performed on a user, a verification method that has not been used to perform verification on the user in predetermined duration prior to a current time is obtained, and then verification is performed on the user by using the obtained verification method. Therefore, using a same verification method to verify the user multiple times in a short period of time is avoided, and user experience is improved.

**[0097]** In another embodiment of the present disclosure, as shown in FIG. 5, step S402 includes the following steps.

**[0098]** In step S501, a verification method list is obtained.

**[0099]** There are multiple rows in the verification method list. Each row includes at least one verification method, and verification methods included in any two rows are not completely the same. If a row includes multiple verification methods, any two verification methods in the row are different.

**[0100]** For example, the verification method list can be shown in Table 6. There are three rows in Table 6. The first row includes two verification methods: short message service message-based verification and email-based verification. The second row includes one verification method: facial verification. The third row includes two verification methods: email-based verification and security question verification.

**Table 6**

|                                                                               |
|-------------------------------------------------------------------------------|
| Short message service message-based verification and email-based verification |
| Facial verification                                                           |
| Email-based verification and security question verification                   |

5 [0101] In step S502, a verification method that has been used to perform verification on the user in the predetermined duration prior to the current time is removed from the verification method list.

[0102] The present step can be specifically implemented in the following processes, including:

[0103] (21) Obtain a correspondence between a verification method and a verification time.

10 [0104] In this embodiment of the present disclosure, each time the server performs verification on the user by using a certain verification method, the server obtains a current local time and uses the current local time as the verification time of performing verification on the user, and then searches the locally stored correspondence between a verification method and a verification time to determine  
15 whether the verification method exists.

[0105] When the correspondence does not include the verification method, it indicates that the verification method has not been previously used to perform verification on the user. In this case, the verification method and the verification time are stored as one record in the correspondence.

20 [0106] When the correspondence includes the verification method, it indicates that the verification method has been previously used to perform verification on the user. In this case, the correspondence needs to be searched for a verification time corresponding to the verification method, and then the obtained verification time is substituted for the identified verification time, so that the verification time of  
25 performing verification on the user by using the verification method can be updated.

[0107] As such, if a latest verification time of previously performing verification on the user in a certain verification method needs to be searched for, the server can obtain the locally stored correspondence between a verification method and a verification time, and then search the correspondence for a verification time  
30 corresponding to the verification method, so as to obtain the latest verification time of

previously performing verification on the user in the verification method.

**[0108]** For example, the correspondence between a verification method and a verification time can be shown in Table 7.

**Table 7**

| Verification method                              | Verification time |
|--------------------------------------------------|-------------------|
| Email-based verification                         | 09:09:22          |
| Short message service message-based verification | 13:05:27          |
| Facial verification                              | 12:08:12          |
| Security question verification                   | 11:32:45          |
| Fingerprint verification                         | 13:01:21          |

5

**[0109]** As shown in Table 7, previously, verification methods that have been used to perform verification on the user include email-based verification, short message service message-based verification, facial verification, security question verification, and fingerprint verification. The latest verification time of performing verification on the user via email-based verification is 09:09:22, the latest verification time of performing verification on the user via short message service message-based verification is 13:05:27, the latest verification time of performing verification on the user via facial verification is 12:08:12, the latest verification time of performing verification on the user via security question verification is 11:32:45, and the latest verification time of performing verification on the user via fingerprint verification is 13:01:21.

10

15

**[0110]** (22) Search the correspondence for a verification method corresponding to a verification time, where a difference between the verification time and the current time is smaller than the predetermined duration.

**[0111]** A verification time included in any record in the correspondence is obtained. The verification time is subtracted from the current time to obtain duration. The duration is compared with the predetermined duration. If the duration is smaller than the predetermined duration, a verification method included in the record is obtained and is used as a verification method corresponding to a verification time, where a difference between the verification time and the current time is smaller than

20

25

the predetermined duration.

[0112] The described operation is performed on any other record in the correspondence. As such, all verification methods corresponding to verification times are identified from the correspondence, where a difference between the verification  
5 time and the current time is smaller than the predetermined duration.

[0113] For example, the current time is 13:10:04, and the predetermined duration is 10 minutes. Verification times 13:05:27 and 13:01:21 can be identified from the correspondence shown in Table 7, where a difference between the verification time and the current time 13:10:04 is smaller than 10 minutes, and it can be determined  
10 that verification methods corresponding to the two verification times are respectively short message service message-based verification and fingerprint verification.

[0114] (23) Delete the identified verification method from the verification method list.

[0115] Specifically, the verification method list is searched for any verification  
15 method identified in step (22). When the verification method list includes the verification method, the verification method is deleted from the verification method list. The described operation is performed for any other verification method identified in step (22). As such, all verification methods identified in step (22) are deleted from the verification method list.

[0116] For example, in the example in step (22), identified verification methods  
20 are short message service message-based verification and fingerprint verification. The verification method list shown in Table 6 is searched for short message service message-based verification, and it is determined that the verification method list shown in Table 6 includes short message service message-based verification. In this  
25 case, short message service message-based verification is deleted from the verification method list shown in Table 6, to obtain a verification method list shown in Table 8.

**Table 8**

|                                                             |
|-------------------------------------------------------------|
| Email-based verification                                    |
| Facial verification                                         |
| Email-based verification and security question verification |

[0117] Then the verification method list shown in Table 8 is searched for fingerprint verification, and it is determined that the verification method list shown in Table 8 does not include fingerprint verification. In this case, the verification method list shown in Table 8 is determined as a post-removal verification method list.

5 [0118] In step S503, a verification method in one row in a post-removal verification method list is obtained.

[0119] The purpose of the present disclosure is to determine one row from the verification method list and perform verification on the user by using all verification methods in the determined row. After the user is verified in all the verification  
10 methods in the determined row, the server can determine that the user is currently verified.

[0120] Therefore, in this embodiment of the present disclosure, the server can actively select one row from the post-removal verification method list. For example, the server can randomly select one row from the post-removal verification method list,  
15 and then obtain all verification methods in the selected row.

[0121] In another embodiment of the present disclosure, the server can send the post-removal verification method list to the terminal, so that the terminal displays the post-removal verification method list to the user. The user can select one row from the post-removal verification method list displayed by the terminal. The terminal sends  
20 the row selected by the user to the server. The server obtains a verification method in the row selected by the user.

[0122] The server can determine that the user is currently verified only after the user is verified in all verification methods in one row in the verification method list. Therefore, if the user selects a row that includes only one verification method, the user  
25 can be currently verified if the user is verified by that verification method. If the user selects a row that includes multiple verification methods, the user can be currently verified only if the user is verified by the multiple verification methods separately. Therefore, the user usually selects a row that includes fewer verification methods from the post-removal verification method list, so that the user can be  
30 currently verified as soon as possible.

[0123] For example, in the post-removal verification method list shown in Table 8, the first row and the second row include fewer verification methods, but the third row includes more verification methods. Therefore, the user usually selects the first row or the second row to be currently verified.

[0124] Therefore, in the present step, if the server actively selects one row from the post-removal verification method list, the server can select a row that includes fewer verification methods, so that the user can be currently verified as soon as possible.

5 [0125] As described in the previous embodiment, the user can be currently verified once the user is verified in all verification methods in any row in the verification method list. Therefore, to ensure the user be currently verified as soon as possible, in another embodiment of the present disclosure, after step S502, as shown in FIG. 6, the method further includes the following steps.

10 [0126] In step S601, it is determined whether the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list.

[0127] In some situations, if all verification methods in a certain row in the verification method list are verification methods in which the user is verified in the  
15 predetermined duration prior to the current time, all the verification methods in the row are removed in step S502, that is, the row is no longer included in the verification method list. As such, the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list.

[0128] For example, if verification methods that have been used to perform  
20 verification on the user in the predetermined duration prior to the current time are short message service message-based verification and facial verification, after step S502, that is, after short message service message-based verification and facial verification are removed from the verification method list shown in Table 6, a verification method list shown in Table 9 can be obtained.

25 **Table 9**

|                                                             |
|-------------------------------------------------------------|
| Email-based verification                                    |
| Email-based verification and security question verification |

[0129] There are two rows in the verification method list shown in Table 9, but there are three rows in the pre-removal verification method list in Table 6. As such, it can be determined that the number of rows in the post-removal verification method  
30 list is smaller than the number of rows in the pre-removal verification method list.

Then step S602 is performed.

**[0130]** In step S602, when the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list, it is determined that the user is currently verified.

5 **[0131]** In this embodiment of the present disclosure, the user can be currently verified once the user is verified in all verification methods in any row in the verification method list. Therefore, once it is determined that the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list, it indicates that the user is verified in all  
10 verification methods in any one of removed rows in the predetermined duration prior to the current time. Therefore, no verification needs to be performed on the user, and it can be determined that the user is currently verified. The process ends.

**[0132]** When the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, step S503 is  
15 performed: Obtain a verification method in one row in a post-removal verification method list.

**[0133]** In this embodiment of the present disclosure, when the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, verification methods in one row may include  
20 verification methods in another row in the post-removal verification method list, that is, the row includes the verification methods in the another row, but the number of verification methods in the row is greater than the number of verification methods in the another row.

**[0134]** For example, in the verification method list shown in Table 8, verification  
25 methods in the third row are email-based verification and security question verification, and a verification method in the first row is email-based verification. The third row includes email-based verification in the first row, and the number of verification methods in the third row is greater than the number of verification methods in the first row. Therefore, the verification methods in the third row include  
30 the verification method in the first row.

**[0135]** The user can be currently verified once the user is verified via email-based verification if the user selects the first row, but the user can be currently verified only when the user is verified via both email-based verification and security question verification if the user selects the third row. Therefore, the user usually prefers the

first row to the third row to be currently verified as soon as possible.

[0136] However, the server may sometimes actively select one row from the post-removal verification method list. If the server selects the third row instead of the first row, the user needs to be verified via both email-based verification and security question verification. In this case, the user cannot be currently verified as soon as possible.

[0137] Therefore, in this embodiment of the present disclosure, when the number of rows in the post-removal verification method list is equal to the number of rows in the pre-removal verification method list, the server determines whether verification methods in any row in the post-removal verification method list include verification methods in another row. When the verification methods in the row include verification methods in another row, the server deletes the row from the post-removal verification method list. The server performs the described operation on any other row.

[0138] For example, the third row is deleted from the verification method list shown in Table 8, to obtain a verification method list shown in Table 10. When selecting one row from the verification method list shown in Table 10, besides selecting the second row that includes facial verification, the server can select the first row that includes email-based verification, and the server cannot select the original third row that includes email-based verification and security question verification in Table 8. As such, the server performs verification on the user only via email-based verification, and the user can be currently verified once the user is verified via email-based verification. Therefore, the user can be verified as soon as possible, and verification efficiency is increased.

**Table 10**

|                          |
|--------------------------|
| Email-based verification |
| Facial verification      |

[0139] Further, in the described embodiment of the present disclosure, after the server performs verification on the user by using an unused verification method, the server obtains a current local time and uses the current local time as a verification time of performing verification on the user by using the unused verification method, and then substitutes, in the locally stored correspondence between a verification

method and a verification time, the verification time for a verification time corresponding to the verification method, so that the verification time of performing verification on the user by using the verification method can be updated.

**[0140]** FIG. 7 is a block diagram illustrating a verification device according to an exemplary embodiment. Referring to FIG. 7, the device includes: a first current time acquisition module 11, configured to: when verification needs to be performed on a user, obtain a current local time; a first verification method acquisition module 12, configured to obtain a verification method in which the user failed to gain verification in predetermined duration prior to the current time; and a first verification module 13, configured to perform verification on the user by using the verification method in which the user failed to gain verification.

**[0141]** In the existing technology, a server performs verification on an identity of a user via short message service message-based verification each time the user performs a sensitive operation. If the user performs multiple sensitive operations in a short period of time, the server performs verification on the user multiple times by using the same verification method in a short period of time, resulting in relatively low user experience.

**[0142]** In this embodiment of the present disclosure, when verification needs to be performed on a user, a verification method in which the user failed to gain verification in predetermined duration prior to a current time is obtained, and then verification is performed on the user by using the obtained verification method. Therefore, using a same verification method to verify the user multiple times in a short period of time is avoided, and user experience is improved.

**[0143]** The first verification method acquisition module 12 includes: a first verification method list acquisition unit, configured to obtain a verification method list, where each row in the verification method list includes at least one verification method; a first removal unit, configured to remove, from the verification method list, a verification method in which the user is verified in the predetermined duration prior to the current time; and a first verification method acquisition unit, configured to obtain a verification method in one row in a post-removal verification method list.

**[0144]** The first removal unit includes: a first acquisition subunit, configured to obtain a locally stored correspondence between a verification method and a passing time; a first search subunit, configured to search the correspondence for a verification method corresponding to a passing time, where a difference between the passing time

and the current time is smaller than the predetermined duration; and a first deletion subunit, configured to delete the identified verification method from the verification method list.

5     **[0145]**     The device further includes: a passing time acquisition module, configured to: when the user is verified in the verification method in which the user is previously unverified, obtain a current local time and determine the current local time as a passing time when the user is verified in the verification method in which the user is previously unverified; and a first substitution module, configured to substitute, in the correspondence, the determined passing time for a passing time corresponding to the  
10    verification method in which the user is previously unverified.

**[0146]**     The first verification method acquisition module 12 further includes: a first judging unit, configured to determine whether the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list; and a first determining unit, configured to: when the number  
15    of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list, determine that the user is currently verified.

**[0147]**     The first verification method acquisition unit is further configured to: when the number of rows in the post-removal verification method list is equal to the  
20    number of rows in the pre-removal verification method list, perform the step of obtaining a verification method in one row in a post-removal verification method list.

**[0148]**     FIG. 8 is a block diagram illustrating a verification device according to an exemplary embodiment. Referring to FIG. 8, the device includes: a second current time acquisition module 21, configured to: when verification needs to be performed  
25    on a user, obtain a current local time; a second verification method acquisition module 22, configured to obtain a verification method that has not been used to perform verification on the user in predetermined duration prior to the current time; and a second verification module 23, configured to perform verification on the user by using the unused verification method.

30    **[0149]**     In the existing technology, a server performs verification on an identity of a user via short message service message-based verification each time the user performs a sensitive operation. If the user performs multiple sensitive operations in a short period of time, the server performs verification on the user multiple times by using the same verification method in a short period of time, resulting in relatively

low user experience.

**[0150]** In this embodiment of the present disclosure, when verification needs to be performed on a user, a verification method that has not been used to perform verification on the user in predetermined duration prior to a current time is obtained, and then verification is performed on the user by using the obtained verification method. Therefore, using a same verification method to verify the user multiple times in a short period of time is avoided, and user experience is improved.

**[0151]** The second verification method acquisition module 22 includes: a second verification method list acquisition unit, configured to obtain a verification method list, where each row in the verification method list includes at least one verification method; a second removal unit, configured to remove, from the verification method list, a verification method that has been used to perform verification on the user in the predetermined duration prior to the current time; and a second verification method acquisition unit, configured to obtain a verification method in one row in a post-removal verification method list.

**[0152]** The second removal unit includes: a second acquisition subunit, configured to obtain a locally stored correspondence between a verification method and a verification time; a second search subunit, configured to search the correspondence for a verification method corresponding to a verification time, where a difference between the verification time and the current time is smaller than the predetermined duration; and a second deletion subunit, configured to delete the identified verification method from the verification method list.

**[0153]** The device further includes: a verification time acquisition module, configured to: when verification is performed on the user by using the unused verification method, obtain a current local time and determine the current local time as a verification time of performing verification on the user by using the unused verification method; and a second substitution module, configured to substitute, in the correspondence, the determined verification time for a verification time corresponding to the unused verification method.

**[0154]** The second verification method acquisition module 22 further includes: a second judging unit, configured to determine whether the number of rows in the post-removal verification method list is smaller than the number of rows in the pre-removal verification method list; and a second determining unit, configured to: when the number of rows in the post-removal verification method list is smaller than

the number of rows in the pre-removal verification method list, determine that the user is currently verified.

**[0155]** The second verification method acquisition unit is further configured to: when the number of rows in the post-removal verification method list is equal to the  
5 number of rows in the pre-removal verification method list, perform the step of obtaining a verification method in one row in a post-removal verification method list.

**[0156]** For the device in the embodiment, a specific method that each module performs an operation has been described in detail in the related method embodiment, and details are not described herein.

10 **[0157]** A person skilled in the art can easily figure out another implementation solution of the present disclosure after considering the specification and practicing the present disclosure. The present application is intended to cover any variations, functions, or adaptive changes of the present disclosure. These variations, functions, or adaptive changes comply with general principles of the present disclosure, and  
15 include common knowledge or a commonly used technical means in the technical field that is not disclosed in the present disclosure. The specification and the embodiments are merely considered as examples, and the actual scope and the spirit of the present disclosure are indicated by the following claims.

**[0158]** It should be understood that the present disclosure is not limited to the  
20 accurate structures that are described above and that are shown in the accompanying drawings. Modifications and changes can be made within the scope of the present disclosure. The scope of the present disclosure is limited only by the appended claims.

## CLAIMS

1. A computer-implemented method, comprising:

recording times and corresponding verification methods of successful user identity verifications;

identifying one or more verification methods of successful user identity verifications performed in a predetermined time period based on the recorded times and corresponding verification methods;

determining whether at least one verification method is included in both the identified one or more verification methods of successful user identity verifications and a list of available verification methods by comparing the identified one or more verification methods of successful user identity verifications with the list of available verification methods, wherein comparing the identified one or more verifications methods of successful user identity verifications with the list of available verification methods comprises deleting a verification method from the list of available verification methods if the verification method is included in the identified one or more verification methods;

determining that additional user identity verification is unnecessary if at least one verification method is included in both the identified one or more verification methods of successful user identity verifications and the list of available verification methods, wherein the list of available verification methods include one or more rows, each row includes at least one verification method, and the additional user identity verification is unnecessary when a row of the list is deleted after deleting the verification method from the list of available verification methods; and

using one or more available verification methods different from the identified one or more verification methods for user identity verification if no verification method is included in both the identified one or more verification methods of successful user identity verifications and the list of available verification methods, wherein using one or more available verification methods different from the identified one or more verification methods for user identity verification further comprises:

randomly selecting a row from the one or more rows after deleting the verification method from the list of available verification methods if the verification method is included in the identified one or more verification methods; or

selecting a row from the one or more rows that has the least number of verification methods after deleting the verification method from the list of available verification methods if the verification method is included in the identified one or more verification methods; and  
using each verification method included in the selected row to perform user identity verification.

2. The computer-implemented method of claim 1, wherein the one or more verification methods include at least one of an e-mail verification, text message verification, biometric verification, and security question verification.

3. The computer-implemented method of claim 1, wherein the list of available verification methods is locally stored on a server.

4. The computer-implemented method of claim 1, further comprises:  
identifying a verification method included in the identified one or more verification methods of successful user identity verifications that is not included in the list of available verification methods; and  
adding the verification method to the list of available verification methods.

5. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform the method of any one of claims 1 to 4.

6. A computer-implemented system, comprising:  
one or more computers; and  
one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform the method of any one of claims 1 to 4.