

SYSTEM AND METHOD FOR USER IDENTITY VERIFICATION, AND CLIENT AND SERVER BY USE THEREOF

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefits to Chinese Patent Application No. 201510082444.9, filed on Feb. 15, 2015, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present invention relates generally to the technologies of network security, and more particularly to a system and method for user identity verification.

BACKGROUND

[0003] In the Internet world, oftentimes serviced by the services provided by service providers, clients need to interact with the servers by which the service providers utilize to provide such services. Typically, it is after the service provider servers verify the identities of the users of the client end that the users are permitted to access the service from the client end.

[0004] The prior art technology verifies a user's identity through prompting the user to answer the security questions or challenges configured upon the registration of the account. If the user answers the security challenges with the right answers pre-configured by the user, it is determined that the user's identity is successfully verified.

[0005] However, there are several problems existing with the prior art technology. For example, the right answers are pre-configured by the user for the security challenges either at the time of user registration or subsequently during the user's normal business operation under the account. The answers configured manually in this manner can easily be decrypted such that unauthorized parties can use the decrypted answers to pass the server verification of the user identity. Once an unauthorized party bypasses the user identity verification of a server, accesses to the respective services configured for the comprised account can be obtained, consequently causing economic harm to the genuine account holder.

[0006] Therefore, there exists a need of a method of user identity verification to enhance user account security.

SUMMARY

[0007] According to an exemplary embodiment of the present disclosure, a method of user identity verification by a server, where the server pre-configures, by use of collected user

information, verification information corresponding to accounts of users in a user verification information data store, the verification information including a plurality of verification security challenges and a plurality of respective first verification answers, includes detecting a condition to whether initiate a user identity verification is satisfied, where an account ID of a user is obtained from the condition. The method also includes inquiring the pre-configured user verification information about verification information matching the account ID and transmitting security challenges of the inquired verification information to the client. The method further includes receiving from the client second verification answers corresponding to the security challenges and comparing the second verification answers with the first verification answers to determine whether the user's identity is verified.

[0008] According to another exemplary embodiment of the present disclosure, a method of user identity verification by a client includes transmitting a triggering request to a server upon receiving a triggering command, the triggering request comprising an account ID of a user. The method also includes receiving from the server security challenges of verification information corresponding to the account ID, the verification information comprising security challenges and corresponding first verification answers generated by the server based on collected user information. The method further includes obtaining second verification answers corresponding to the received security challenges and transmitting the second verification answers to the server, where the server compares the second verification answers with the corresponding first verification answers to determine whether the user's identity is verified.

[0009] According to yet another exemplary embodiment of the present disclosure, a method of user identity verification by a client includes receiving from a server security challenges of verification information, the verification information comprising security challenges and corresponding first verification answers generated by the server based on collected user information. The method also includes obtaining second verification answers corresponding to the received security challenges and transmitting the second verification answers to the server, where the server compares the second verification answers with the corresponding first verification answers to determine whether a user's identity is verified.

[0010] According to still yet another exemplary embodiment of the present disclosure, a system for user identity verification includes a server and a client. The server is configured to pre-configure, by use of collected user information, verification information corresponding to accounts of users in a user verification information data store, the verification information including a plurality of verification security challenges and a plurality of respective first verification answers, receive from the client a triggering request, the triggering request including

an account ID of a user, inquire the pre-configured user verification information about verification information matching the account ID, transmit security challenges of the inquired verification information to the client, receive from the client second verification answers corresponding to the security challenges, and compare the second verification answers with the first verification answers to determine whether the user's identity is verified. The client is configured to transmit to the server the triggering request, receive from the server the security challenges, obtain the second verification answers corresponding to the security challenges, and transmit the second verification answers to the server.

[0011] According to an exemplary embodiment of the present disclosure, a system for user identity verification includes a server and a client. The server is configured to pre-configure, by use of collected user information, verification information corresponding to accounts of users in a user verification information data store, the verification information including a plurality of verification security challenges and a plurality of respective first verification answers, detect a user's operations under an account meeting a pre-configured triggering condition, inquire the pre-configured user verification information about verification information matching an account ID of the user, transmit security challenges of the inquired verification information to the client, receive from the client second verification answers corresponding to the security challenges, and compare the second verification answers with the first verification answers to determine whether the user's identity is verified. The client is configured to receive from the server the security challenges, obtain the second verification answers corresponding to the security challenges, and transmit the second verification answers to the server.

[0012] According to yet another exemplary embodiment of the present disclosure, a server for user identity verification includes a pre-configuration module configured to pre-configure, by use of collected user information, verification information corresponding to accounts of users in a user verification information data store, the verification information including a plurality of verification security challenges and a plurality of respective first verification answers. The server also includes an inquiring and transmitting module configured to inquire the pre-configured user verification information about verification information matching an account ID of a user and to transmit security challenges of the inquired verification information to a client, where the inquiring and transmitting module is executed upon an initiating condition being met. The server further includes a receiving module configured to receive from the client second verification answers corresponding to the security challenges and a comparison module configured to compare the second verification answers with the first verification answers to determine whether the user's identity is verified.

[0013] According to still another exemplary embodiment of the present disclosure, a client for user identity verification includes a first transmitting module configured to, upon receiving a triggering command, transmit to a server a triggering request, the triggering request including an account ID of a user. The client also includes a receiving module configured to receive from the server security challenges of verification information corresponding to the account ID, the verification information comprising security challenges and corresponding first verification answers generated by the server based on collected user information. The client further includes an obtaining module configured to obtain second verification answers corresponding to the security challenges and a second transmitting module configured to transmit to the server the second verification answers, where the server compares the second verification answers with the corresponding first verification answers to determine whether a user's identity is verified.

[0014] According to still yet another exemplary embodiment of the present disclosure, a client for user identity verification includes a receiving module configured to receive from the server security challenges of verification information, the verification information comprising security challenges and corresponding first verification answers generated by the server based on collected user information. The client further includes an obtaining module configured to obtain second verification answers corresponding to the security challenges and a transmitting module configured to transmit to the server the second verification answers, where the server compares the second verification answers with the corresponding first verification answers to determine whether a user's identity is verified.

DESCRIPTION OF THE DRAWINGS

[0015] The accompanying drawings, which are incorporated in and form a part of this specification and in which like numerals depict like elements, illustrate embodiments of the present disclosure and, together with the description, serve to explain the principles of the disclosure.

[0016] FIGS. 1A-1B are flow charts of exemplary methods of user identity verification illustrated from the perspective of a server in accordance with an embodiment of the present disclosure;

[0017] FIG. 2 is an illustration of a ROC curve of determining whether a security challenge is an optimal solution security challenge;

[0018] FIG. 3 is a flow chart of another exemplary method of user identity verification illustrated from the perspective of a server in accordance with an embodiment of the present disclosure;

[0019] FIG. 4 is a flow chart of an exemplary method of user identity verification corresponding to the exemplary method of FIG. 1A and illustrated from the perspective of a client in accordance with an embodiment of the present disclosure;

[0020] FIG. 5 is a flow chart of an exemplary method of user identity verification corresponding to the exemplary method of FIG. 3 and illustrated from the perspective of a client in accordance with an embodiment of the present disclosure;

[0021] FIG. 6 is a block diagram of an exemplary system for user identity verification in accordance with an embodiment of the present disclosure;

[0022] FIG. 7 is a block diagram of an exemplary server for user identity verification in accordance with an embodiment of the present disclosure;

[0023] FIG. 8 is a system block diagram of another exemplary server for user identity verification in accordance with an embodiment of the present disclosure;

[0024] FIG. 9 is a system block diagram of an exemplary client for user identity verification in accordance with an embodiment of the present disclosure; and

[0025] FIG. 10 is a system block diagram of another exemplary client for user identity verification in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0026] In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. However, it will become obvious to those skilled in the art that the present disclosure may be practiced without these specific details. The descriptions and representations herein are the common means used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. In other instances, well-known methods, procedures, components, and circuitry have not been described in detail to avoid unnecessarily obscuring aspects of the present disclosure.

[0027] Reference herein to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one embodiment of the disclosure. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Used herein, the terms “upper”, “lower”, “top”, “bottom”, “middle”, “upwards”, and “downwards” are intended to provide relative positions for the purposes of description, and are not intended to designate an absolute frame of reference. Further, the order of blocks in

process flowcharts or diagrams representing one or more embodiments of the disclosure do not inherently indicate any particular order nor imply any limitations in the disclosure.

[0028] Embodiments of the present disclosure are discussed herein with reference to FIGS. 1A-10. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the disclosure extends beyond these limited embodiments.

[0029] Referring to FIG. 1A, a flow chart of an exemplary method of user identity verification is shown in accordance with embodiments of the present disclosure. The method 100 starts in step S110, where a server pre-configures verification information of an account of a user in a user verification information data store based on the collected user information. The verification information includes verification security challenges and corresponding first verification answers. The server collects information from the user during the routine operations thereof. By use of the collected user information, the server can pre-configure account verification information for the user in the user verification information data store. The verification information includes a plurality of verification security challenges and a plurality of corresponding first verification answers.

[0030] In some embodiments, the collected user information is the account information of the user such as, for example, the information of the user's Alipay account. Correspondingly, the pre-configured verification information can have the verification information including the security challenges such as "how much is the balance of the present Alipay account" and "how much is the profit of the present month under the Yu'E Bao account", etc. Correspondingly, the first verification answer, i.e., the right answers, can be "\$20,000" and "\$74.1", respectively. Further, one of ordinary skills in the art will readily appreciate from this example that, at different points of time, there are different first verification answers, i.e., the right answers corresponding to the same security challenges. In other words, the first verification answers are dynamic and vary from time to time.

[0031] In some other embodiments, the collected user information is the operation information with regard to how the user operates the account. For example, the last operation the user performed under his or her Taobao account. In this case, the security challenges of the pre-configured verification information can be "what is the user's last login time for the Taobao account" and "what is the user's last login address for the Taobao account", etc. Correspondingly, the first verification answers can be "Jan. 26, 2015" and "Suzhou", respectively.

[0032] In some other embodiments, the collected user information is the information with regard to the user's mobile terminal. For example, the information of the user's cell phone device. In this case, the verification security challenges of the pre-configured verification information can be the information regarding the mobile terminal device of the user such as, for example, "what is the brand and model of the last cell phone the user owned". Correspondingly, the first verification answer can be "Xiaome 2S".

[0033] In some embodiments, in order to enhance the reliability of the method of user identity verification provided by the present disclosure, different verification information can be pre-configured in the user verification information data store for business scenarios at different risk level. Such verification information can be different in terms of the content of the verification security challenges, the number of verification security challenges, or both. For example, risk levels for business scenarios can be classified into three categories: a high risk (e.g., the second time verification of a payment passcode, a medium risk (e.g., the second time verification of user login), and low risk (e.g., unlinking a bank debit card). Accordingly, for the high risk category, the verification information can include 6 verification security challenges, the medium risk 5, and the low risk 3.

[0034] In step S120, the server receives a triggering request from a user, the triggering request including an account ID of the user. In real world business scenarios, if the user wants to perform corresponding business operations under an account registered at a web site, the user can send a triggering request from the client to the server. For example, when the user wants to modify the login passcode for an on-line bank account or to perform a transaction of transfer to another account from an on-line bank account, the user can send a request of changing passcode or a request of bank transfer from a client to a server of the corresponding on-line bank, respectively. For another example, if the user wants to tether a different mobile device to an on-line bank account, the user can send a tethering-switch request from the client to the server of the on-line bank. For yet another example, shopping at the web site of "Taobao" or using the web site of "Fanli" to shop at the web site of "Taobao", the user can utilize an Alipay account to transact payments for the merchandise purchased online, sending a payment request from a client to an Alipay server.

[0035] A client from which a user sends a triggering request includes, but not limited to, any fixed terminal, smart terminal, and mobile terminal. For example, such a client can be a laptop computer, desktop computer, set-top box, PDA (personal digital assistant), cellular device, iPhone, smartphone, iPad, iWatch, etc.

[0036] The triggering request received by the server can include an account ID of the user.

[0037] In step S130, the server inquires the pre-configured verification information about the verification information corresponding to the account ID included in the received triggering request, and transmits the verification security challenges of the corresponding verification information to the client.

[0038] Upon receiving a triggering request, the server can utilize the account ID of the user included in the triggering request to inquire the pre-configured verification information about the verification information corresponding to the triggering request. After obtaining the corresponding verification information, the server transmits the verification security challenges to the client.

[0039] In some embodiments, in step S110, various verification information can be pre-configured accordingly for various real world business risk scenarios. Upon receiving a trigger request from a client, the server determines the risk level corresponding to the received triggering request. Subsequently, the determined risk level is utilized by the server to inquire about the verification information that corresponds to the determined risk scenario level, the verification information including the verification security challenges as well as respective first verification answers. For example, when receiving a triggering request to unlink a bank debit card from an Alipay account, the server determines that the present risk scenario is in the category of low risk. Correspondingly, the inquired security challenges can be, for example, “what is the cellular number pre-stored at the bank of the debt card linked to the present Alipay account?”, or “what is the passcode for the Alipay account tethered to the present bank debit card?”, etc. Accordingly, the first verification answers can be, for example, “139xxxxxxx”, and “xxxxxx”, etc.

[0040] In step S140, the server receives from the client the second verification answers, i.e., user’s responses, corresponding to the verification security challenges.

[0041] Upon receiving the verification security challenges from the server, the client obtains the second verification answers corresponding to the received security challenges, and transmits the obtained second verification security answers to the server. The second verification security answers obtained by the client includes, but not limited to, the second verification answers entered by the user in real time response to the security challenges and then obtained by the client, or the second security answers pre-configured by the user and obtained by the client.

[0042] For example, the client can obtain the second verification answers entered by the user in real time response to the security challenges by, after receiving the verification security challenges from the server, displaying the received security challenges to the user, upon which

the user views the displayed security challenges and subsequently enters the second verification answers.

[0043] For another example, the client can obtain the second verification answers pre-configured by the user by, pre-establishing a verification security answer store, which includes various second verification answers configured by the user. After receiving the verification security challenges from the server, the client terminal inquires the security answer store about the corresponding second verification answers.

[0044] In general, for n number of verification security challenges, there are n number of second verification answers; although there are cases where there are less than n number of second verification answers corresponding to the n number of challenges.

[0045] In step S150, the server compares the received second verification answers to the first verification answers, the result of which is utilized to determine whether the present user's identity can be successfully verified. After receiving the second verification answers from the client, the server compares the received second verification answers with the first verification answers of the verification information obtained before, and determines whether the present user's identity can be verified based on the result of the comparison.

[0046] When the second verification answers match the first verification answers, it is determined that the present user's identity is successfully verified. When the second verification answers don't match the first verification answers, it is determined that the present user's identity is not verified. The matching of the second verification answers with the first verification answers can be that the second verification answers are identical to the first verification answers; or the second verification answers include contents that are substantially identical to the first verification answers. For example, for a second verification answer "January 26, 2016", it matches a first verification answer "2015-1-26" with substantially identical contents.

[0047] It should be pointed out that, in cases of a single verification security challenge, it can be determined that the present user's identity is verified when the corresponding second verification answer matches the first verification answer. But, in cases of multiple verification security challenges, various criteria can be implemented to determine whether the present user's identity can be verified. For example, a criterion can be that, when each of the second verification security answers matches the corresponding first verification answer, it is determined that the present user's identity is verified; or it can be based on whether the result of the comparison of the second verification answers with the first verification answers meets a pre-configured mapping standard. If the result of comparing the second verification answers with the first verification answers meets the pre-configured mapping standard, it is determined that the

present user's identity is verified. Otherwise, it is determined that the present user's identity is not verified.

[0048] The above described mapping standard can be, for example, "2 matches out of 3 comparisons", "3 matches out of 5 comparisons", etc. In details, when there are 3 verification security challenges, a "2 matches of 3 comparisons" standard can be utilized to determine whether the present user's identity can be verified. If at least 2 out a total of 3 second verification answers match the corresponding first verification answers, it is determined that the present user's identity is successfully verified. When there are 5 verification security challenges, a "3 matches of 5 comparisons" standard can be utilized to determine whether the present user's identity can be verified. If at least 3 out a total of 5 second verification answers match the corresponding first verification answers, it is determined that the present user's identity is successfully verified. Further, different mapping standards can be configured for risk scenarios at different levels. For example, a "2 matches of 3 comparisons" standard can be configured for a low risk scenario where a bank debit card is to be unlinked.

[0049] In some other embodiments, the step S150 can also include steps S151-S152 (FIG. 1B) to enhance the reliability of positive verification of a user's identity. In step S151, a probability of a second verification answer matching a corresponding first verification answer is computed by use of a pre-configured algorithm. The pre-configured algorithm can be a prior art algorithm, an improved prior art algorithm, or an algorithm defined specifically under the circumstances. The matching probability can be a probability that the user is a genuine self when the second verification answers match the corresponding first verification answers; or the matching probability can be a probability that the user is a genuine self when the second verification answers don't match the corresponding first verification answers.

[0050] In cases where there is a single verification security challenge, the matching probability is a probability that the user is genuine with regard to the single verification security challenge. In cases where there are multiple verification security challenges, the matching probability is a probability that the user is genuine with regard to all the verification security challenges.

[0051] In step S152, the computed matching probability is compared to a pre-configured threshold value such that to determine whether the present user's identity can be verified. Different threshold values can be pre-configured at the server according to different risk levels of the business scenarios. For example, in a high risk scenario where a payment passcode is verified for the second time, a threshold value can be pre-configured at about 95%. For a medium risk scenario where the user attempts to login for the second time, a threshold value can

be pre-configured at about 80%. For a low risk scenario where a bank debit card is unlinked, a threshold value can be pre-configured at about 50%.

[0052] Based on the result of the comparison of the computed matching probability with the pre-configured threshold value, it is determined whether the present user's identity can be verified. If the matching probability equals or exceeds the pre-configured threshold value, it is determined that the present user's identity is verified. If the matching probability does not exceed the pre-configured threshold value, it is determined that the present user's identity is not verified. Once the user's identity is not verified, either the user cannot perform any subsequent operations, or the user has to utilize other alternative identity verification methods to be verified again.

[0053] For example, a user A performs payment passcode verification for the second time. If the computed matching probability for the user A is 83.36%, which is apparently much lower than a pre-configured threshold value 95%, the user A is deemed not verified for the second time regarding payment passcode verification. If the user A instead performs login verification for the second time, and if the computed matching probability for the user A is the same 83.36%, which is higher than a pre-configured threshold value 80%, the user A is deemed verified for the second time regarding login verification.

[0054] By use of computing a probability of the second verification answers matching the corresponding first verification answers, and comparing the computed matching probability with a pre-configured threshold value, the present disclosure provides for enhanced reliability for positive verification of user identities.

[0055] In some other embodiments, the user verification information data store referred in the step S110 also includes input information that corresponds to the stored verification information. The input information includes computation parameters for computing a matching probability between a second verification answer and a first verification answer. Computation parameters can include a first probability of a second verification answer provided by a user matching a corresponding first verification answer, and a second probability of such second verification answer not matching the corresponding first verification answer. Computation parameters can further include a third probability of a second verification answer not provided by the user matching the corresponding first verification answer, and a fourth probability of such second verification answer not matching the corresponding first verification answer. In other words, computation parameters include the probabilities of a genuine user answering the verification security challenges correctly and wrongly, and users answering the verification security challenges correctly and wrongly. Answers to the corresponding security challenges

pertaining to the user is considered security answers provided by the genuine user self. Answers to the corresponding security challenges pertaining to someone who is not the user is considered security answers provided by another user.

[0056] One exemplary way to obtain the above described computational parameters is through user testing. An exemplary user test can be that, first, every participating tester answers his or her own verification security challenges and others' verification security challenges. Next, statistics are computed for the number of times each participating tester answers correctly his or her own security challenges, the number of times each participating tester answers wrongly his or her own security challenges, the number of times each participating tester answers correctly others' security challenges, and the number of times each participating tester answers wrongly others' security challenges. Last, corresponding probabilities are computed as computation parameters. For example, for a security challenge "what is the model of the last mobile device owned", computation parameters obtained through user testing can be computed as the following:

Table 1

	Answer Correctly	Answer Wrongly
Self	92%	8%
Non-self	10%	90%

For different security challenges, corresponding computation parameters can be different.

[0057] Further, in some embodiments, the above described security challenge can be an optimal solution security challenge. One of the standards to measure the performance quality of a security challenge is that the probability a user self answering it correctly is high, and at the same time the probability of other users answering it correctly is low. To quantify this standard, after obtaining the computation parameters for a security challenge by user testing, a graph of ROC curve is generated in a coordination having a x axis of FPR (False Positive Rate), i.e., the probability of other users (non-self) answering the security challenge correctly and a y axis of TPR (True Positive Rate), i.e., the probability of a user self answering the security challenge correctly. Referring to FIG. 2, an exemplary graph 200 of a ROC curve 202 is shown in accordance with embodiments of the present disclosure. The ROC curve 202 is generated based on the probability data of "self answering correctly" and "non-self answering correctly" collected from the security challenges defined by the businesses and having the best recognition probability. Point T_0 falls to the upper left side of the ROC curve 202, the security challenge represented by T_0 is considered an optimal security challenge. Point T_1 falls to the upper right

side of the ROC curve 202, the security challenge represented by T_1 is considered an inferior security challenge. By use of selecting optimal security challenges that maximize the probability of a user self answering correctly and minimize the probability of other users answering correctly, the risks of imposter users being verified as authorized users can be lowered for business services.

[0058] Correspondingly, in the step S151, a matching probability of a second verification answer matching the corresponding first verification answer can be computed by use of an algorithm in the following. For a set of n security challenges, an i th probability of the second verification answer corresponding to the i th security challenge matching the corresponding first verification answer is computed. The i th probability is designated as the $i+1$ th pretest probability, which is utilized to compute the $i+1$ th probability of the corresponding first verification answers of the $i+1$ th security challenge matching the corresponding first verification answer. Here, i is an integer within the range of $1-n$. The i th matching probability includes an i^+ th probability of the second verification answer corresponding to the i th security challenge matching the corresponding first verification answer, or an i^- th probability of the second verification answer corresponding to the i th security challenge not matching the corresponding first verification answer.

[0059] In particular, the first matching probability of a second verification answer to the first security challenge matching the corresponding first verification answer is computed by use of a pre-configured pretest probability. Next, the computed first matching probability is designated as the second pretest probability, which is utilized to compute the second matching probability of a second verification answer to the second security challenge matching the corresponding first verification answer. Following how the second matching probability is computed, the remaining $n-2$ matching probabilities are computed respectively for a second verification answer to the corresponding security challenge matching the corresponding first verification answer, the corresponding security challenge is one of the remaining $n-2$ security challenges in the set of n security challenges. When the n th matching probability of a second verification answer to the corresponding n th security challenge matching the corresponding first verification answer is computed, the last matching probability is computed and the computing of matching probability is done.

[0060] Correspondingly, in step S152, the computed n th matching probability is compared to a pre-configured threshold value such that to determine whether the user's identity can be verified. In some embodiments, for the i th security challenge, when the second verification

answer is correct, the probability of the user being genuine (the i^{+} th probability) can be computed by formula (1):

$$P_i(\text{self} | \text{right}) = \frac{P_i(\text{right} | \text{self}) * P_i(\text{self})}{P_i(\text{right} | \text{non-self}) * P_i(\text{non-self}) + P_i(\text{right} | \text{self}) * P_i(\text{self})} \quad (1)$$

For the same i th security challenge, when the second verification answer is wrong, the probability of the user still being genuine (the i th probability) can be computed by formula (2):

$$P_i(\text{self} | \text{wrong}) = \frac{P_i(\text{wrong} | \text{self}) * P_i(\text{self})}{P_i(\text{wrong} | \text{non-self}) * P_i(\text{non-self}) + P_i(\text{wrong} | \text{self}) * P_i(\text{self})} \quad (2)$$

[0061] In the above two formulas, $P_i(\text{self} | \text{right})$ is the i^{+} th matching probability of a second verification answer to the i th security challenge matching the corresponding first verification answer; $P_i(\text{right} | \text{self})$ is the first probability corresponding to the i th security challenge; $P_i(\text{right} | \text{non-self})$ is the third probability corresponding to the i th security challenge; $P_i(\text{self} | \text{wrong})$ is the i th non-matching probability of a second verification answer to the i th security challenge not matching the corresponding first verification answer; $P_i(\text{wrong} | \text{self})$ is the second probability corresponding to the i th security challenge; $P_i(\text{wrong} | \text{non-self})$ is the fourth probability corresponding to the i th security challenge; and $P_i(\text{self})$ is the i th pretest probability, the value of which is the i -th matching probability, and $P_i(\text{non-self}) = 1 - P_i(\text{self})$.

[0062] For the first security challenge, $P_1(\text{self})$ and $P_1(\text{non-self})$ can be each configured as 50%. Also, answering correctly refers to a second verification answer matching the corresponding first verification answer; answering wrongly refers to a second verification answer not matching the corresponding first verification answer. In cases there are multiple security challenges, the computed matching probability of the present security challenge is designated as the pretest probability for the next security challenge. For a set of n security challenges, the n th computed matching probability is the final matching probability of the second verification answers matching the corresponding first verification answers.

[0063] For example, a user A answers three security challenges, the correctness of the answers are shown in Table 2, in which “correct” refers to that the second verification answer matches the corresponding first verification answer, and “wrong” refers to that the second verification answer does not match the corresponding first verification answer.

Table 2

	Security challenge 1	Security challenge 2	Security challenge 3
User A	correct	wrong	correct

[0064] The three security challenges have the computational parameters configured as the same, which is shown in Table 3.

Table 3

	Correct	wrong
Self	95%	5%
Non-self	10%	90%

[0065] When the first security challenge 1 is answered correctly, the probability that the user A is the user himself or herself can be computed by the formula (3):

$$\begin{aligned}
 P_1(\text{self}|\text{right}) &= \frac{P_1(\text{right}|\text{self}) * P_1(\text{self})}{P_1(\text{right}|\text{non-self}) * P_1(\text{non-self}) + P_1(\text{right}|\text{self}) * P_1(\text{self})} \quad (3) \\
 &= \frac{95\% * 50\%}{10\% * 50\% + 95\% * 50\%} \\
 &= 90.47\%
 \end{aligned}$$

Next, the computed $P_1(\text{self}|\text{right})$ is designated as $P_2(\text{self})$ in the following formula (4), which is utilized to compute the probability that the user A is himself or herself when the security challenge 2 is answered wrongly:

$$\begin{aligned}
 P_2(\text{self}|\text{wrong}) &= \frac{P_2(\text{wrong}|\text{self}) * P_2(\text{self})}{P_2(\text{wrong}|\text{non-self}) * P_2(\text{non-self}) + P_2(\text{wrong}|\text{self}) * P_2(\text{self})} \quad (4) \\
 &= \frac{5\% * 90.47\%}{90\% * 9.53\% + 5\% * 90.47\%} \\
 &= 34.53\%
 \end{aligned}$$

Next, $P_2(\text{self}|\text{wrong})$ is designated as $P_3(\text{self})$ in the following formula (5), which is utilized to compute the probability that the user A is himself or herself when the security challenge 3 is answered correctly:

$$\begin{aligned}
P_3(\text{self}|\text{right}) &= \frac{P_3(\text{right}|\text{self}) * P_3(\text{self})}{P_3(\text{right}|\text{non-self}) * P_3(\text{non-self}) + P_3(\text{right}|\text{self}) * P_3(\text{self})} \quad (5) \\
&= \frac{95\% * 34.53\%}{10\% * 65.47\% + 95\% * 34.53\%} \\
&= 83.36\%
\end{aligned}$$

[0066] Last, the probability of the user A being genuine is 83.36%, i.e., for those three security challenges, the matching probability of the second verification answers matching the corresponding first verification answers is 83.36%.

[0067] In some other embodiments, computational parameters can also include a pre-configured probability for each security challenge. The pre-configured probabilities can be the same or different. Correspondingly, in step S151, a matching probability of second verification answers matching the corresponding first verification answers can be computed by use of an algorithm in the following. For a set of n security challenges, by use of a pre-configured probability, an initial i th probability of a second verification answer corresponding to the i th security challenge matching the corresponding first verification answer is computed for each of the security challenge. Next, by use of pre-configured algorithms, a final probability of the second verification answers matching the corresponding first verification answers is computed with all the initial probabilities corresponding to all the security challenges. An initial probability can be a probability that a user is genuine, including a first initial probability of the second verification answer matching the corresponding first verification answer and a second initial probability of the second verification answer not matching the corresponding first verification answer.

[0068] In the step S152, the computed final matching probability is compared to a pre-configured threshold value such that to determine whether the user's identity can be verified. In some embodiments, the initial probability for each security challenge can be computed by formula (6) or formula (7):

$$P(\text{self} | \text{right}) = \frac{P(\text{right} | \text{self}) * P(\text{self})}{P(\text{right} | \text{non-self}) * P(\text{non-self}) + P(\text{right} | \text{self}) * P(\text{self})} \quad (6)$$

$$P(\text{self} | \text{wrong}) = \frac{P(\text{wrong} | \text{self}) * P(\text{self})}{P(\text{wrong} | \text{non-self}) * P(\text{non-self}) + P(\text{wrong} | \text{self}) * P(\text{self})} \quad (7)$$

[0069] $P(\text{self} | \text{right})$ is the first initial probability of a second verification answer corresponding to each security challenge matching the corresponding first verification answer;

$P(\text{right} | \text{self})$ is the first probability corresponding to each security challenge;
 $P(\text{right} | \text{non-self})$ is the third probability corresponding to each security challenge;
 $P(\text{self} | \text{wrong})$ is the second initial probability of a second verification answer corresponding to each security challenge not matching the corresponding first verification answer;
 $P(\text{wrong} | \text{self})$ is the second probability corresponding to each security challenge;
 $P(\text{wrong} | \text{non-self})$ is the fourth probability corresponding to each security challenge; and
 $P(\text{self})$ is the pre-configured probability corresponding to each security challenge,
 $P(\text{non-self}) = 1 - P(\text{self})$. The first, second, third, and fourth probabilities of each security challenge can be the same or different.

[0070] As to the pre-configured algorithms which are utilized to compute the final probability, an exemplary algorithm can be an average of all the computed initial probabilities corresponding to all the security challenges, or an expected value of all the initial probabilities corresponding to all the security challenges. Such algorithms are not limited to the above described, any algorithm that computes a reasonable final probability over the initial probabilities is within the scope of the present disclosure.

[0071] Further, the two above described pre-configured algorithms to compute the matching probability of the second verification answers matching the corresponding first verification answers are also exemplary without limiting the scope of the present disclosure.

[0072] Referring to FIG. 3, a flow chart of another method of user identity verification is shown in accordance with embodiments of the present disclosure. Method 300 starts in step S310, which is substantially similar to the step S110 of FIG. 1A and the details are not repeated here for the purpose of simplicity.

[0073] In step S320, the server detects that the user operates the account to meet a triggering condition, after which the server inquires about the verification information corresponding to the account ID of the user, and transmits the security challenges of the inquired verification information to the client of the user.

[0074] Triggering conditions can be that the server detects that the user performs certain business operations under the account. For example, the user logs into the Taobao account from the cell phone to modify the passcode for the Taobao account, or the user logs into the Alipay account from a Fanli account. Triggering conditions can also be that the server detects a terminal change at the user's end. For example, the server detects that the user is logging into the account utilizing a cell phone of a model different than the model utilized in the last login, or the server detects that the user logs into the account from a foreign address, or the server detects

that the devices utilized by the user are abnormal in general or not recognized specifically for the user by the server.

[0075] The server can obtain the account ID by analyzing the account information of the user. The step of inquiring the pre-configured verification information about the verification information corresponding to the account ID of the user and the transmitting of the inquired verification information to the user at the client is substantially similar to the step S130, and the details are not repeated here for the purpose of simplicity.

[0076] In step S330, the server receives the second verification answers corresponding to the security challenges from the client. In step S340, the server compares the received second verification answers to the corresponding first verification answers such that to determine whether the user's identity can be verified. The details of the steps S330 and S340 are substantially similar to those of the steps S140 and S150, and therefore not repeated here for the purpose of simplicity.

[0077] The above described verification information is pre-configured based on the user information collected by the server. Therefore, such verification information cannot be easily comprehended by imposter users and contributes to enhanced user account security. Further, by use of configuring different security challenges based on business scenarios at different risk levels, computing the matching probabilities of multiple second verification answers matching the corresponding first verification answers, configuring different threshold values based on different business scenarios at different risk levels, and comparing the computed matching probability with the pre-configured threshold value to determine whether the user's identity can be verified, the reliability of positive verification of user identify can be enhanced.

[0078] Referring to FIG. 4, a flow chart of a method of verifying user identity corresponding to FIG. 1A and illustrated from a client's perspective is shown in accordance with embodiments of the present disclosure. Method 400 starts in step S410, where upon receiving a triggering command, the client transmits to a server the received triggering command, the triggering command including an account ID of the user.

[0079] A triggering command can be that the user logs into the account from a web site that does not host the account, for example, the user logs into the Alipay account from the Fanli web site. A triggering command can also be that the user performs business operations under the account, for example, the user transacts bank transfers under an online bank account. A triggering command can also be that the user logs into the account from a foreign address or a device that is abnormal in general or not recognized specifically for the user by the server. The

account ID can be obtained from the account information of the user by the client upon receiving the triggering command.

[0080] In step S420, the client receives from the server the security challenges of the verification information corresponding to the account ID of the user, the verification information including the security challenges generated by the server based on the collected user information and corresponding first verification answers.

[0081] In step S430, the client obtains the second verification answers corresponding to the security challenges. After receiving from the server the security challenges, the client obtains the second verification answers to the security challenges. Similar to those described in the step S140, the second verification answers obtained at the client can be entered in real time by the user at the client in response to the security challenges, or it can be the user pre-configured verification answers that are retrieved by the client.

[0082] In step S440, the client transmits to the server the obtained second verification answers. The server receives the second verification answers and compares to the corresponding first verification answers such that to determine whether the present user's identity can be verified.

[0083] Referring to FIG. 5, a flow chart of a method of verifying user identity corresponding to FIG. 3 and illustrated from a client's perspective is shown in accordance with embodiments of the present disclosure. Method 500 starts in step S510, where the client receives from the server the security challenges of the verification information, the verification information including the security challenges generated by the server based on the collected user information and the corresponding first verification answers.

[0084] In step S520, the client obtains the second verification information corresponding to the received security challenges. In step S530, the client transmits the obtained second verification answers to the server to request the server to compare the second verification answers with the corresponding first verification answers and to determine whether the present user's identity can be verified. Other details are substantially similar to those of the steps S420-S440 and not repeated here for the purpose of simplicity.

[0085] Referring to FIG. 6, a block diagram of a system for verifying user identification is shown in accordance with embodiments of the present disclosure. The system 600 includes a server 601 and a client 602. In some embodiments, the server 601 is configured to collect users' information and pre-configure the verification information corresponding to a user's account in a user verification information data store. The verification information includes security challenges and corresponding first verification answers. The server 601 is also configured to

receive triggering requests from the client, the triggering request including an account ID of the user and to inquire the pre-configured user verification information about the verification information corresponding to the account ID. The server 601 is further configured to transmit the security challenges of the inquired verification information to the client, to receive from the client the second verification answers corresponding to the security challenges, and to compare the received second verification answers with the corresponding first verification answers to determine whether the present user's identity can be verified.

[0086] The client 602 is configured to transmit a triggering request to the server 601, to receive from the server the security challenges, to obtain the second verification answers corresponding to the security challenges, and to transmit the obtained second verification answers to the server.

[0087] In some other embodiments, in addition to or in place of the server 601 receiving triggering requests from the client, the server 601 is configured to detect whether the user's operations under the account meet a pre-configured triggering condition. When the pre-configured triggering condition is met, the server 601 is configured to inquire the pre-configured user verification information about the verification information corresponding to the account ID of the user. Correspondingly, the client 602 is configured to receive from the server the security challenges, to obtain the second verification answers corresponding to the security challenges, and to transmit the obtained second verification answers to the server.

[0088] Referring to FIG. 7, a block diagram of a server for verifying user identification is shown in accordance with embodiments of the present disclosure. Server 800 includes a pre-configuration module 801, a first receiving module 802, an inquiring and transmitting module 803, a second receiving module 804 and a comparison module 805. The pre-configuration module 801 is configured to collect users' information and pre-configure the verification information corresponding to a user's account in a user verification information data store. The verification information includes security challenges and corresponding first verification answers. The first receiving module 802 is configured to receive triggering requests from the client, the triggering request including an account ID. The inquiring and transmission module 803 is configured to inquire the pre-configured user verification information about the verification information corresponding to the account ID and to transmit the security challenges of the inquired verification information to the client. The second receiving module 804 is configured to receive from the client the second verification answers corresponding to the security challenges. The comparison module 805 is configured to compare the received second

verification answers with the corresponding first verification answers to determine whether the present user's identity can be verified.

[0089] Referring to FIG. 8, a block diagram of another server for verifying user identification is shown in accordance with embodiments of the present disclosure. Server 900 includes a pre-configuration module 901, an inquiring and transmitting module 902, a receiving module 903 and a comparison module 904. The pre-configuration module 901 is configured to collect users' information and pre-configure the verification information corresponding to a user's account in a user verification information data store. The verification information includes security challenges and corresponding first verification answers. The inquiring and transmission module 902 is configured to, upon detecting the user's operations under the account meeting a pre-configured condition, inquire the pre-configured user verification information about the verification information corresponding to the account ID and transmit the security challenges of the inquired verification information to the client. The receiving module 903 is configured to receive from the client the second verification answers corresponding to the security challenges. The comparison module 904 is configured to compare the received second verification answers with the corresponding first verification answers to determine whether the present user's identity can be verified.

[0090] In some embodiments, the pre-configuration module 801 of FIG. 7 and the pre-configuration module 901 of FIG. 8 are further configured to pre-configure in the user verification information data store input information corresponding to the verification information, the input information including computation parameters for computing matching probabilities of second verification answers matching corresponding first verification answers.

[0091] Exemplary computation parameters include a first probability of a second verification answer provided by a user self matching the corresponding first verification answer, a second probability of such user self verification answer not matching the corresponding first verification answer, a third probability of a second verification answer provided by other users matching the corresponding first verification answer, and a fourth probability of such other user second verification answer not matching the corresponding first verification answer.

[0092] In some embodiments, the comparing module 805 of FIG. 7 and the comparing module 904 of FIG. 8 include a computing sub-module and a comparison sub-module (not shown). The computing sub-module is configured to computing the matching probability of the second verification answers matching the corresponding first verification answers by use of a pre-configured algorithm. The comparison sub-module is configured to compare the computed matching probability with a pre-configured threshold value to determine whether the present

user's identity can be verified. Exemplary matching probabilities can be a probability that the user is genuine when second verification answers match the corresponding first verification answers, or a probability that the user is genuine when second verification answers do not match the corresponding first verification answers.

[0093] In some embodiments, the computing sub-module includes a first computing sub-module, a second computing sub-module and a third computing sub-module. The first computing sub-module is configured to compute a first probability of a second verification answer to the first security challenge matching the corresponding first verification answer by use of a pre-configured pretest probability. The second computing sub-module is configured to designate the computed first probability as the second pretest probability, and to compute a second probability of the a second verification answer to the second security challenge matching the corresponding first verification answer by use of the second pretest probability. The third computing sub-module is configured to repeat the process of computing the second probability to compute the remaining $n-2$ probabilities of a second verification answer matching the corresponding first verification answer, each second verification answer corresponding to each of the remaining $n-2$ security challenges, until the n th probability is computed for the n th security challenge. In the cases where there is a single security challenge, only the first computing sub-module is executed to compute the matching probability of a second verification answer to a security challenge matching the corresponding first verification answer. In the cases where there are two security challenges, both the first computing sub-module and the second computing sub-module are executed to compute the matching probability of second verification answers to security challenges matching the corresponding first verification answers.

[0094] Correspondingly, the comparison sub-module includes a first comparison sub-module configured to compare the n th probability with a pre-configured threshold value.

[0095] In some other embodiments, the computing sub-module includes an initial computing sub-module configured to compute an initial matching probability of a second verification answer to each security challenge matching the corresponding first verification answer by use a pre-configured probability. The computing sub-module also includes a final computing sub-module configured to compute a final matching probability with all the initial matching probabilities for all the security challenges by use of a pre-configured algorithm.

[0096] Correspondingly, the comparison sub-module includes a second comparison sub-module configured to compare the computed final matching probability with a pre-configured threshold value.

[0097] Referring to FIG. 9, a block diagram of a client for verifying user identification is shown in accordance with embodiments of the present disclosure. Client 1000, corresponding to the server 800, includes a first transmitting module 1001, a receiving module 1002, an obtaining module 1003 and a second transmitting module 1004. The first transmitting module 1001 is configured to transmit to the server a triggering request, the triggering request including an account ID of the user. The receiving module 1002 is configured to receive from the server security challenges of the verification information corresponding to the account ID, the verification information including the security challenges generated by the server based on the collected user information and the corresponding first verification answers. The obtaining module 1003 is configured to obtain second verification answers corresponding to the security challenges. The second transmitting module 1004 is configured to transmit to the server the obtained second verification answers and to request the server to compare the second verification answers to the corresponding first verification answers such that to determine whether the present user's identity can be verified.

[0098] Referring to FIG. 10, a block diagram of another client for verifying user identification is shown in accordance with embodiments of the present disclosure. Client 1100, corresponding to the server 900, includes a receiving module 1101, an obtaining module 1102 and a transmitting module 1103. The receiving module 1101 is configured to receive from the server security challenges of the verification information corresponding to the account ID, the verification information including the security challenges generated by the server based on the collected user information and the corresponding first verification answers. The obtaining module 1102 is configured to obtain second verification answers corresponding to the security challenges. The transmitting module 1103 is configured to transmit to the server the obtained second verification answers and to request the server to compare the second verification answers to the corresponding first verification answers such that to determine whether the present user's identity can be verified.

[0099] Embodiments of the present disclosure can be implemented using software, hardware, firmware, and/or the combinations thereof. Regardless of being implemented using software, hardware, firmware or the combinations thereof, instruction code can be stored in any kind of computer readable media (for example, permanent or modifiable, volatile or non-volatile, solid or non-solid, fixed or changeable medium, etc.). Similarly, such medium can be implemented using, for example, programmable array logic (PAL), random access memory (RAM), programmable read only memory (PROM), read only memory (ROM), electrically erasable

programmable ROM (EEPROM), magnetic storage, optical storage, digital versatile disc (DVD), or the like.

[00100] It is necessary to point out that, modules or blocks described by embodiments of the present disclosures are logical modules or logical blocks. Physically, a logical module or logical block can be a physical module or a physical block, a part of a physical module or a physical block, or the combinations of more than one physical modules or physical blocks. Physical implementation of those logical module or logical blocks is not of essence. The realized functionalities realized by the modules, blocks and the combinations thereof are key to solving the problems addressed by the present disclosure. Further, in order to disclose the novelties of the present disclosure, the above described embodiments do not disclose about those modules or blocks not too related to solving the problems addressed by the present disclosure, which does not mean that the above described embodiments cannot include other modules or blocks.

[00101] It is also necessary to point out that, in the claims and specification of the present disclosure, terms such as first and second only are for distinguishing an embodiment or an operation from another embodiment or operation. It does not require or imply that those embodiments or operations having any such real relationship or order. Further, as used herein, the terms “comprising,” “including,” or any other variation intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Absent further limitation, elements recited by the phrase “comprising a” does not exclude a process, method, article, or apparatus that comprises such elements from including other same elements.

[00102] While the foregoing disclosure sets forth various embodiments using specific block diagrams, flowcharts, and examples, each block diagram component, flowchart step, operation, and/or component described and/or illustrated herein may be implemented, individually and/or collectively, using a wide range of hardware, software, or firmware (or any combination thereof) configurations. In addition, any disclosure of components contained within other components should be considered as examples because many other architectures can be implemented to achieve the same functionality.

[00103] The process parameters and sequence of steps described and/or illustrated herein are given by way of example only and can be varied as desired. For example, while the steps illustrated and/or described herein may be shown or discussed in a particular order, these steps do not necessarily need to be performed in the order illustrated or discussed. The various

example methods described and/or illustrated herein may also omit one or more of the steps described or illustrated herein or include additional steps in addition to those disclosed.

[00104] While various embodiments have been described and/or illustrated herein in the context of fully functional computing systems, one or more of these example embodiments may be distributed as a program product in a variety of forms, regardless of the particular type of computer-readable medium used to actually carry out the distribution. The embodiments disclosed herein may also be implemented using software modules that perform certain tasks. These software modules may include script, batch, or other executable files that may be stored on a computer-readable storage media or in a computing system. These software modules may configure a computing system to perform one or more of the example embodiments disclosed herein. One or more of the software modules disclosed herein may be implemented in a cloud computing environment. Cloud computing environments may provide various services and applications via the Internet. These cloud-based services (e.g., software as a service, platform as a service, infrastructure as a service, etc.) may be accessible through a Web browser or other remote interface. Various functions described herein may be provided through a remote desktop environment or any other cloud-based computing environment.

[00105] Although the present disclosure and its advantages have been described in detail, it should be understood that various changes substitutions, and alterations can be made herein without departing from the spirit and scope of the disclosure as defined by the appended claims. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the disclosure and its practical applications, to thereby enable others skilled in the art to best utilize the disclosure and various embodiments with various modifications as may be suited to the particular use contemplated.

[00106] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present disclosure, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed, that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present disclosure. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

[00107] Embodiments according to the present disclosure are thus described. While the present disclosure has been described in particular embodiments, it should be appreciated that the disclosure should not be construed as limited by such embodiments, but rather construed according to the below claims.

CLAIMS

1. A method of user identity verification by a server, the server pre-configuring, by use of collected user information, verification information corresponding to accounts of users in a user verification information data store, the verification information including a plurality of verification security challenges and a plurality of respective first verification answers, the method comprising the steps of:
- detecting whether a condition to initiate a user identity verification is satisfied, wherein an account ID of a user is obtained from the condition;
- if the condition to initiate a user identity verification is satisfied, then inquiring the pre-configured user verification information about verification information matching the account ID;
- transmitting security challenges of the inquired verification information to a client;
- receiving, from the client, a plurality of second verification answers corresponding to the security challenges; and
- comparing the second verification answers with the first verification answers to determine whether the user's identity is verified, wherein, the comparing the second verification answers with the first verification answers to determine whether the user's identity is verified comprises the steps of:
- computing a matching probability of the second verification answers matching the first verification answers by use of a pre-configured algorithm; and
- comparing the computed matching probability with a pre-configured threshold value to determine whether the user's identity is verified;
- characterised in that
- the step of computing a matching probability of the second verification answers matching the first verification answers comprises the step of:
- a) computing a first matching probability of a second verification answer to a first security challenge of the plurality of security challenges matching a corresponding first verification answer by use of a pre-

configured first pretest probability, wherein the second verification answer is one of the plurality of second verification answers, and the corresponding first verification answers is one of the plurality of first verification answers;

5 b) designating the computed matching probability as a pretest probability;

 c) computing a next matching probability of a next second verification answer to a next security challenge of the plurality of security challenges matching a corresponding first verification answer by use of the pretest probability, wherein the next second verification answer is one of the plurality of second verification answers, and the corresponding first verification answer is one of the plurality of first verification answers; and

 d) repeating steps b) and c) until a last matching probability of a last second verification answer to a last security challenge of the plurality of security challenges matching a corresponding first verification answer is computed, wherein the last second verification answer is one of the plurality of second verification answers, and the corresponding first verification answer is one of the plurality of first verification answers,

20 wherein the step of comparing the computed matching probability to the pre-configured threshold value comprises comparing the last matching probability with the pre-configured threshold value, and wherein during the repeating of steps b) and c) the pretest probability of each step b) is used as the pretest probability of the next step c).

25 2. The method of claim 1, wherein the condition comprises detecting one or more operations of the user under the account meeting a triggering pre-condition.

 3. The method of claim 1, wherein the verification information pre-configured in the user verification information data store comprises input information pre-configured for the verification information, the input information comprising a computation

30

parameter utilized to compute the matching probability between the first verification answers and the second verification answers.

4. The method of claim 3, wherein the computation parameter comprises:
 - 5 a first probability of a second verification answer provided by the user matching a corresponding first verification answer; and
 - a second probability of the second verification answer provided by the user not matching the corresponding first verification answer.
- 10 5. The method of any preceding claim, wherein a first verification answer of the plurality of first verification answers is dynamically determined in part by data associated with one or more accounts of the user, the data subject to changes.
6. A server for user identity verification, the server comprising:
 - 15 a processor; and
 - a non-transitory computer-readable medium operably coupled to the processor, the non-transitory computer-readable medium having computer-readable instructions stored thereon to be executed when accessed by the processor, the instructions comprising:
 - 20 a pre-configuration module configured to pre-configure, by use of collected user information, verification information corresponding to accounts of users in a user verification information data store, the verification information including a plurality of verification security challenges and a plurality of respective first verification answers;
 - 25 an inquiring and transmitting module configured to inquire the pre-configured user verification information about verification information matching an account ID of a user and to transmit security challenges of the inquired verification information to a client, wherein the inquiring and transmitting module is executed upon an initiating condition being met;

a receiving module configured to receive from the client a plurality of second verification answers corresponding to the security challenges; and

a comparison module configured to compare the second verification answers with the first verification answers to determine whether the user's identity is verified, wherein the comparison module comprises:

a computing sub-module configured to, by use of a pre-configured algorithm, compute a matching probability of the second verification answers matching the first verification answers; and

a comparison sub-module configured to compare the computed matching probability with a pre-configured threshold value to determine whether the user's identity is verified;

characterised in that the computing sub-module is configured to:

a) compute a first matching probability of a second verification answer to a first security challenge of the plurality of security challenges matching a corresponding first verification answer by use of a pre-configured first pretest probability, wherein the second verification answer is one of the plurality of second verification answers, and the corresponding first verification answers is one of the plurality of first verification answers;

b) designate the computed matching probability as a pretest probability;

c) compute a next matching probability of a next second verification answer to a next security challenge of the plurality of security challenges matching a corresponding first verification answer by use of the pretest probability, wherein the next second verification answer is one of the plurality of second verification answers, and the corresponding first verification answer is one of the plurality of first verification answers; and

d) repeat b) and c) until a last matching probability of a last second verification answer to a last security challenge of the plurality of security challenges matching a corresponding first verification answer is computed, wherein the last second verification answer is one of the plurality of second

verification answers, and the corresponding first verification answer is one of the plurality of first verification answers,

wherein the comparison sub-module is configured to compare the last matching probability with the pre-configured threshold value, and wherein during the repeating of
5 b) and c) the pretest probability of each b) is used as the pretest probability of the next c).

7. The server of claim 6, further comprising a request receiving module configured to receive a triggering request from the client, the triggering request including the
10 account ID of the user, wherein the initiating condition is met upon the request receiving module receiving the triggering request.

8. The server of claim 6 or claim 7, wherein the initiating condition is met upon detecting one or more operations of the user under the account meeting a pre-configured
15 triggering condition.

9. The server of any of claims 6 to 8, wherein a first verification answer of the plurality of first verification answers is dynamically determined in part by data associated with one or more accounts of the user, the data subject to changes.