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;

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,

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).

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

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:

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.

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:

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:

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;

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 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 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 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.