

Claims

1. A computer-implemented method for risk identification, the method being executed by one or more processors and comprising:

receiving , by the one or more processors, a user input comprising identification information of a user requesting a service, a definition of a type of the service, and an identifier of a provider of the service;

processing, by the one or more processors, a first portion of the identification information to determine a first address coding information representing code values associated with first address information associated with the user, wherein the first address coding information comprises a fraud grade and a server risk grade, wherein the fraud grade is associated with the identification information and the fraud grade comprises a ratio of fraud cases related to the first address within a time interval relative to a total number of fraud cases per service provider within the time interval, and wherein the server risk grade is associated with a number of server terminals through which the user applies for services within the time interval;

retrieving, by the one or more processors, a second address coding information based on a second portion of the identification information , wherein the second address coding information represents coding values associated with second address information associated with the user, wherein the identification information comprises fuzzified identification information;

matching, by the one or more processors, the first address coding information with the second address coding information to generate an address matching result;

determining, by the one or more processors, a risk identification result associated with the user based on the address matching result and a service scenario code corresponding to the service that the user is requesting;

transmitting, by the one or more processors, the risk identification result associated with the user to a server terminal of the service that the user is requesting;

receiving, by the one or more processors, information on whether to regulate a processing operation of the service, the information determined at the server terminal of the service that the user is requesting based upon the risk identification result associated with the user; and

based on the information on whether to regulate a processing operation of the service, selectively processing or blocking the processing operation of the service.

2. The method according to claim 1, wherein the first address coding information and the second address coding information are address information which is identified by adopting numbers, letters, or numbers and letters.
3. The method according to claim 1, wherein determining the risk identification result according to the address matching result comprises:
 - when the address matching result is that the first address coding information is not consistent with the second address coding information, determining that the service requested by the user currently has a risk.
4. The method according to claim 1, wherein the service is a network transaction service, the first address associated with the first address coding information is a billing address and a second address associated with the second address coding information is a logistic shipping address.
5. The method according to claim 1, further comprising:
 - retrieving first credit record information corresponding to the first address coding information and second credit record information corresponding to the identification information; and
 - determining risk rating information of the user used for determining risk identification result based on the first credit record information and the second credit record information.
6. The method according to claim 5, wherein the first credit record information comprises at least one of:
 - address validity grade information of the first address indicated in the first address coding information;
 - information indicating whether a fraud case related to the first address occurs within a recent first set time length; and
 - information indicating at least one of occurrence times of fraud cases related to the first address within a recent second set time length, amounts of fraud cases related to the first address within a recent second set time length, and a quantity proportion of such cases in all fraud cases,

wherein the recent first set time length is smaller than the recent second set time length.

7. The method according to claim 5, wherein the second credit record information comprises at least one of:

information indicating whether the user is a blacklist user, the blacklist user being a user having a bad credit record;

information indicating whether the user has an association with a blacklist user;

information indicating whether the user has an association with a user having a fraud behavior within a recent third set time length;

information indicating whether the user has a fraud behavior or whether the user has an association with a fraud case; and

information indicating the number of server terminals through which the user applies for services within a recent fourth set time length.

8. The method according to any one of claims 5-7, wherein the services are pre-loan application services or online application crediting services and wherein the second credit record information comprises information indicating the number of server terminals through which the user applies for services within a recent fourth set time length.

9. The method according to claim 1, further comprising:

receiving an address coding request carrying the first address;

determining coding values respectively corresponding to address contents at each level obtained after division according to a stored corresponding relation between address contents at different levels and coding values and the address contents at each level obtained by dividing the first address, wherein a geographical range corresponding to an address content at a level which is not a lowest contains a plurality of geographical ranges corresponding to address contents at a level lower than the level; and

arranging the coding values respectively corresponding to the address contents at each level obtained after division in an order from a largest to a smallest corresponding to the address contents of the levels to form an address coding value corresponding to the first address, and feeding back address coding information containing the address coding value.

10. The method according to claim 9, wherein the address coding information further contains address validity grade information; and

the address validity grade information is determined by:

determining an affiliation relation between address contents at different levels in the first address based on the coding values respectively corresponding to the address contents at each level in the first address and a stored superior-subordinate relation between different coding values; and

determining the address validity grade information of the first address according to the affiliation relation and invalid address contents, in the first address, which have no corresponding relation with the coding values.

11. An apparatus for address matching-based risk identification, comprising:

a receiving module configured to receive a user input comprising identification information of a user requesting a service, a definition of a type of the service, and an identifier of a provider of the service;

a determination module configured to: process a first portion of the identification information to determine a first address coding information representing code values associated with first address information associated with the user, wherein the first address coding information comprises a fraud grade and a server risk grade, wherein the fraud grade is associated with the identification information and the fraud grade comprises a ratio of fraud cases related to the first address within a time interval relative to a total number of fraud cases per service provider within the time interval, and wherein the server risk grade is associated with a number of server terminals through which the user applies for services within the time interval and retrieve a second address coding information based on a second portion of the identification information, wherein the second address coding information represents coding values associated with second address information associated with the user, wherein the identification information comprises fuzzified identification information;

a matching module configured to match the first address coding information with the second address coding information to generate an address matching result and determine a risk

identification result associated with the user based on the address matching result and a service scenario code corresponding to the service that the user is requesting and

a transmission module configured to:

transmit the risk identification result associated with the user to a server terminal of the service that the user is requesting;

receive information on whether to regulate a processing operation of the service, the information determined at the server terminal of the service that the user is requesting based upon the risk identification result associated with the user; and

based on the information on whether to regulate a processing operation of the service, selectively process or blocking the processing operation of the service.

12. The apparatus according to claim 11, wherein the first address coding information and the second address coding information are address information which is identified by adopting numbers and/or letters.

13. The apparatus according to claim 11, wherein the matching module is specifically configured to:

when the address matching result is that the first address is not consistent with the second address, determine that the service requested to be processed by the user currently has a risk.

14. The apparatus according to claim 11, wherein the service is a network transaction service, the first address is a billing address and the second address is a logistic shipping address.

15. The apparatus according to claim 11, wherein the determination module is further configured to:

determine first credit record information corresponding to the first address coding information and second credit record information corresponding to the identification information; and determine risk rating information of the user used for performing risk identification based on the first credit record information and the second credit record information.

16. The apparatus according to claim 15, wherein the first credit record information comprises one or more pieces of the following information:

address validity grade information of the first address indicated in the first address coding information;

information indicating whether a fraud case related to the first address occurs within a recent first set time length; and

information indicating at least one of occurrence times of fraud cases related to the first address within a recent second set time length, amounts of fraud cases related to the first address within a recent second set time length, and a quantity proportion of such cases in all fraud cases, wherein the recent first set time length is smaller than the recent second set time length.

17. The apparatus according to claim 15, wherein the second credit record information comprises one or more pieces of the following information:

information indicating whether the user is a blacklist user, the blacklist user being a user having a bad credit record;

information indicating whether the user has an association with a blacklist user;

information indicating whether the user has an association with a user having a fraud behavior within a recent third set time length;

information indicating whether the user has a fraud behavior or whether the user has an association with a fraud case; and

information indicating the number of server terminals through which the user applies for services within a recent fourth set time length.

18. The apparatus according to any one of claims 15-17, wherein the services are pre-loan application services or online application crediting services; the second credit record information comprises information indicating the number of server terminals through which the user applies for services within a recent fourth set time length; and

the determination module is further configured to:

determine an application degree level, to which the number of server terminals through which the user applies for services within the recent fourth set time length belongs, for performing risk identification.

19. The apparatus according to claim 11, wherein the receiving module is further configured to receive an address coding request carrying the first address; and the determination module is further configured to:

determine coding values respectively corresponding to address contents at each level obtained after division according to a stored corresponding relation between address contents at different levels and coding values and the address contents at each level obtained by dividing the first address, wherein a geographical range corresponding to an address content at a level which is not a lowest contains a plurality of geographical ranges corresponding to address contents at a level lower than the level; and combine the coding values respectively corresponding to the address contents at each level obtained after division in a descending order of the levels to form an address coding value corresponding to the first address, and feed back address coding information containing the address coding value.

20. The apparatus according to claim 19, wherein the address coding information further contains address validity grade information; and

the determination module is further configured to determine the address validity grade information according to the following steps:

determining an affiliation relation between address contents at different levels in the first address based on the coding values respectively corresponding to the address contents at each level in the first address and a stored superior-subordinate relation between different coding values; and

determining the address validity grade information of the first address according to the determined affiliation relation and invalid address contents, in the first address, which have no corresponding relation with the coding values.