

CLAIMS

1. A method for service processing, the method comprising:
receiving a service processing request from a user(S101, S201);
performing a fast risk identification on the service processing request based on an identification algorithm of a fast risk identification layer (S101, S201);
determining, based on the identification algorithm of the fast risk identification, the possibility of identifying whether the service processing request is risky (S102, S201);
in response to determining that the identification algorithm of the fast risk identification is unable to determine whether the service processing request is risky, performing a deep risk identification on the service processing request based on an identification algorithm of a deep risk identification layer, wherein a first data volume used for the deep risk identification is greater than a second data volume used for the fast risk identification, and a first duration of the deep risk identification is greater than a second duration of the fast risk identification (S102, S203); and
processing the service processing request based on a result of the deep risk identification (S103, S204).
2. The method according to claim 1, wherein performing fast risk identification on the service processing request based on the identification algorithm of the fast risk identification layer comprises:
determining, based on user data comprised in the service processing request, whether the user data corresponds to one of a pre-stored trusted user list and a risky user list (S201);
and
in response to determining that the user data corresponds to the trusted user list, determining that the service processing request is safe and in response to determining that the user data corresponds to the risky user list, determining that the service processing request is risky.
3. The method according to claim 2, wherein in response to determining that the user data corresponds to neither the pre-stored trusted user list, nor the pre-stored risky user list, performing fast risk identification on the service processing request based on an identification algorithm of a fast risk identification layer further comprises:

determining, based on the user data comprised in the service processing request, historical behavior data of the user, and a rule model used for user behavior profile comparison, whether current operation behavior of the user indicated by the service processing request matches historical habitual operation behavior of the user; and

in response to determining that the current operation behavior matches the historical habitual operation behavior of the user, determining that the service processing request is safe.

4. The method according to claim 3, wherein in response to determining that the current operation behavior does not match the historical habitual operation behavior of the user, determining that the service processing request is risky.

5. The method according to claim 1, wherein performing deep risk identification on the service processing request based on the identification algorithm of the deep risk identification layer comprises:

selecting at least one risk theme from a plurality of predetermined risk themes based on a service processing type of the service processing request;

selecting, for each selected risk theme based on service scenario information corresponding to the service processing request, a rule model used for deep risk identification; and

performing the deep risk identification on the service processing request based on the selected rule model.

6. The method according to claim 5, wherein the service processing type comprises a fund transfer, a payment, or transmission of virtual currency.

7. The method according to claim 5, wherein the service scenario information comprises an information about transaction types, payment methods, types of logistics, or transaction parties.

8. The method according to claim 7, wherein the information about transaction types comprises an instant transfer or a secured transaction.

9. The method according to claim 7, wherein the payment methods comprise a balance payment, a fast payment, or an e-bank payment.

10. The method according to claim 7, wherein the types of logistics comprise a physical transaction or a virtual transaction.

11. The method according to claim 7, wherein the transaction parties comprise proprietary merchant or a third-party merchant.

12. The method according to any one of claims 1 to 10, wherein the method further comprises:

performing a comprehensive risk identification on the service processing request based on the identification algorithm of the comprehensive risk identification layer, wherein the comprehensive risk identification, the fast risk identification, and the deep risk identification are asynchronously performed, a third data volume used for the comprehensive risk identification is greater than the second data volume used for the fast risk identification and the first data volume used for the deep risk identification, and a third duration of the comprehensive risk identification is greater than the second duration of the fast risk identification and the first duration of the deep risk identification; and

updating one or more of the following information based on a result of the comprehensive risk identification:

- the predetermined trusted user list;
- the predetermined risky user list;
- the historical behavior data of the user; and
- the predetermined rule model.

13. The method according to claim 12, wherein the comprehensive risk identification comprises:

- retrieving an additional user data from another service website of another server,
- calculating a user relationship network data and an accumulated user behavior data; and
- applying the identification algorithm to the additional user data, the user relationship network data, the accumulated user behavior data, first user data used for the fast risk identification and second user data used for the deep risk identification.

14. The method according to any one of claims 1 to 13, wherein the user data comprises one or more of: an internet protocol (IP) address, a media access control (MAC) address, and a terminal location, an application account, and a bankcard number.
15. An apparatus for service processing, the apparatus comprising a plurality of modules configured to perform the method according to any one of claims 1 to 14.