

CLAIMS

What is claimed is:

1. A computer-implemented method for identity verification, comprising:
 - receiving, from a client device, a request for updating an account;
 - in response to receiving the request, obtaining, by a server from the client device, personal information of a user of the client device and information of a network environment associated with client device, wherein the personal information comprises biometric information and account information of the user;
 - performing, by the server, risk identification of the personal information to obtain a first risk identification result, wherein the first risk identification result identifies security risks associated with inconsistencies between the user and an owner of the account;
 - performing, by the server, risk identification of the information of the network environment to obtain a second risk identification result, wherein the second risk identification result identifies security risks associated with the network environment;
 - calculating, by the server, a first risk score based on the account information;
 - calculating, by the server, a second risk score based on the biometric information;
 - calculating, by the server, a third risk score based on the second risk identification result;
 - selecting, by the server, an identity verification method based on the first risk score, the second risk score, and the third risk score; and
 - performing, by the server, identity verification of the user based on the identity verification method.
2. The computer-implemented method according to claim 1, wherein performing risk identification of the information of the network environment comprises:
 - performing feature extraction to extract at least one feature from the information of the network environment; and
 - inputting the at least one feature to a risk control model to perform the risk identification of the information of the network environment.

3. The computer-implemented method according to claim 1, wherein the account information comprises at least one of historical transaction information of the account, historical operation information of the account, or network identity information associated with the account.

4. The computer-implemented method according to claim 3, wherein performing risk identification of the personal information to obtain the first risk identification result comprises performing risk identification of the personal information to obtain the first risk identification result in response to determining that the account information is inconsistent with prestored account information.

5. The computer-implemented method according to claim 1, further comprising:

determining the first risk identification result as risky in response to determining that the biometric information is inconsistent with prestored biometric information.

6. The computer-implemented method according to claim 1, wherein the biometric information comprises one or more of iris information, fingerprint information, voiceprint information, or facial feature information.

7. The computer-implemented method according to claim 1, wherein performing identity verification of the user based on the identity verification method comprises:

inputting the first risk identification result and the second risk identification result to a prestored machine learning model to obtain an identity verification result of the user, wherein the identity verification result identifies a probability that the user is an owner of the account.

8. The computer-implemented method of claim 1, further comprising:

in response to determining that the identity verification of the user is successful, updating the account based on the request.

9. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, from a client device, a request for updating an account;

in response to receiving the request, obtaining, from the client device, personal information of a user of the client device and information of a network environment associated with client device, wherein the personal information comprises biometric information and account information of the user;

performing risk identification of the personal information to obtain a first risk identification result, wherein the first risk identification result identifies security risks associated with inconsistencies between the user and an owner of the account;

performing risk identification of the information of the network environment to obtain a second risk identification result, wherein the second risk identification result identifies security risks associated with the network environment;

calculating a first risk score based on the account information;

calculating a second risk score based on the biometric information;

calculating a third risk score based on the second risk identification result;

selecting an identity verification method based on the first risk score, the second risk score, and the third risk score; and

performing identity verification of the user based on the identity verification method.

10. The non-transitory, computer-readable medium according to claim 9, wherein performing risk identification of the information of the network environment comprises:

performing feature extraction to extract at least one feature from the information of the network environment; and

inputting the at least one feature to a risk control model to perform the risk identification of the information of the network environment.

11. The non-transitory, computer-readable medium according to claim 9, wherein the account information comprises at least one of historical transaction information of the account, historical operation information of the account, or network identity information associated with the account.

12. The non-transitory, computer-readable medium according to claim 11, wherein performing risk identification of the personal information to obtain the first risk identification result comprises performing risk identification of the personal information to obtain the first risk identification result in response to determining that the account information is inconsistent with prestored account information.

13. The non-transitory, computer-readable medium according to claim 9, further comprising:

determining the first risk identification result as risky in response to determining that the biometric information is inconsistent with prestored biometric information.

14. The non-transitory, computer-readable medium according to claim 9, wherein the biometric information comprises one or more of iris information, fingerprint information, voiceprint information, or facial feature information.

15. The non-transitory, computer-readable medium according to claim 9, wherein performing identity verification of the user based on the identity verification method comprises:

inputting the first risk identification result and the second risk identification result to a prestored machine learning model to obtain an identity verification result of the user, wherein the identity verification result identifies a probability that the user is an owner of the account.

16. The non-transitory, computer-readable medium of claim 9, further comprising:

in response to determining that the identity verification of the user is successful, updating the account based on the request.

17. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing

one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

- receiving, from a client device, a request for updating an account;

- in response to receiving the request, obtaining, from the client device, personal information of a user of the client device and information of a network environment associated with client device, wherein the personal information comprises biometric information and account information of the user;

- performing risk identification of the personal information to obtain a first risk identification result, wherein the first risk identification result identifies security risks associated with inconsistencies between the user and an owner of the account;

- performing risk identification of the information of the network environment to obtain a second risk identification result, wherein the second risk identification result identifies security risks associated with the network environment;

- calculating a first risk score based on the account information;

- calculating a second risk score based on the biometric information;

- calculating a third risk score based on the second risk identification result;

- selecting an identity verification method based on the first risk score, the second risk score, and the third risk score; and

- performing identity verification of the user based on the identity verification method.

18. The computer-implemented system according to claim 17, wherein performing risk identification of the information of the network environment comprises:

- performing feature extraction to extract at least one feature from the information of the network environment; and

- inputting the at least one feature to a risk control model to perform the risk identification of the information of the network environment.

19. The computer-implemented system according to claim 17, wherein the account information comprises at least one of historical transaction information of the

account, historical operation information of the account, or network identity information associated with the account.

20. The computer-implemented system according to claim 19, wherein performing risk identification of the personal information to obtain the first risk identification result comprises performing risk identification of the personal information to obtain the first risk identification result in response to determining that the account information is inconsistent with prestored account information.

21. The computer-implemented system according to claim 17, further comprising:

determining the first risk identification result as risky in response to determining that the biometric information is inconsistent with prestored biometric information.

22. The computer-implemented system according to claim 17, wherein the biometric information comprises one or more of iris information, fingerprint information, voiceprint information, or facial feature information.

23. The computer-implemented system according to claim 17, wherein performing identity verification of the user based on the identity verification method comprises:

inputting the first risk identification result and the second risk identification result to a prestored machine learning model to obtain an identity verification result of the user, wherein the identity verification result identifies a probability that the user is an owner of the account.

24. The computer-implemented system of claim 17, further comprising:

in response to determining that the identity verification of the user is successful, updating the account based on the request.