

WHAT IS CLAIMED IS:

1. A method for verifying a security of a service operation, comprising:

generating one or more risk control models based on user data associated with a user of a service terminal;

receiving, by the service terminal, a creditability analysis instruction of the service operation, the creditability analysis instruction being sent by a service server in response to an operation request associated with the service terminal;

performing, by the service terminal, a creditability analysis to obtain a creditability analysis result of the service operation based on the creditability analysis instruction and the one or more risk control models pre-stored in the service terminal; and

sending, by the service terminal, the creditability analysis result to the service server for determining the security of the service operation.
2. The method according to claim 1, further comprising:

obtaining the user data from the service terminal based on an authorization permission of a user of the service terminal;

generating the one or more risk control models by analyzing the user data; and

storing the one or more risk control models in a database of the service terminal.
3. The method according to claim 2, further comprising:

encrypting the one or more risk control models before storing the one or more risk control models in a local security control database of the service terminal; and

storing the encrypted one or more risk control models in the database of the service terminal.

4. The method according to claim 2, wherein the user data comprises at least one of: user social data, interest data and habit data, and wherein the one or more risk control models comprise at least one of: a social relationship control model generated based on the user social data, an interest control model generated based on the interest data, and a habit control model generated based on the habit data.

5. The method according to claim 1, wherein obtaining a creditability analysis result of the service operation comprises:

obtaining service information of the service operation based on the creditability analysis instruction;

obtaining a target risk control model from the one or more risk control models based on a type of the service operation, wherein the one or more risk control models include a corresponding relationship between service information and service creditability analysis values; and

searching the target risk control model by using the service information as a keyword to obtain a service creditability analysis value corresponding to the service information.

6. The method according to claim 5, wherein obtaining service information of the service operation based on the creditability analysis instruction comprises:

obtaining the service information from the creditability analysis instruction of the service operation, wherein the service information includes information obtained by the service server based on an operation request of the service operation sent by another terminal.

7. The method according to claim 5, further comprising:

when a user of the service terminal initiates the service operation, sending an operation request of the service operation to the service server before receiving the creditability analysis instruction; and

when receiving the creditability analysis instruction, obtaining the service information of the service operation based on the operation request of the service operation.

8. A method for verifying a security of a service operation, comprising:

sending a creditability analysis instruction of the service operation to a service terminal in response to an operation request associated with the service terminal;

receiving a creditability analysis result sent by the service terminal, wherein the creditability analysis result is obtained by the service terminal based on the service terminal performing a creditability analysis of the service operation and one or more risk control models pre-stored in the service terminal; and

determining the security of the service operation based on the creditability analysis result.

9. The method according to claim 8, further comprising:

before sending the creditability analysis instruction of the service operation to the service terminal, receiving the operation request of the service operation sent by another terminal; and

obtaining service information of the service operation based on the operation request, wherein the creditability analysis instruction of the service operation includes the service information of the service operation.

10. The method according to claim 8, further comprising:

before sending the creditability analysis instruction of the service operation to the service terminal, receiving the operation request of the service operation sent by the service terminal, wherein the operation request is used as a trigger instruction for sending the creditability analysis instruction of the service operation to the service terminal.

11. The method according to claim 8, wherein determining the security of the service operation based on the creditability analysis result comprises:

obtaining a first creditability analysis value of the service operation based on a local risk control model;

obtaining a second creditability analysis value based on the creditability analysis result sent by the service terminal;

obtaining weight values of the first creditability analysis value and the second creditability analysis value;

calculating a combined creditability analysis value of the first creditability analysis value and the second creditability analysis value based on the weight values;

comparing the combined creditability analysis value with a preset creditability threshold;
and

if the combined creditability analysis value is greater than the creditability threshold, determining that the service operation is secure, and if the combined creditability analysis value is not greater than the creditability threshold, determining that the service operation is insecure.

12. A device for verifying a security of a service operation, comprising:

a generating unit configured to generate one or more risk control models based on user data associated with a user of a service terminal;

a receiving unit configured to receive a creditability analysis instruction of the service operation sent by a service server;

an analyzing unit configured to obtain a creditability analysis result of the service operation based on the service terminal performing a creditability analysis and the one or more risk control models pre-stored in the service terminal; and

a sending unit configured to send the creditability analysis result to the service server for determining the security of the service operation.

13. A device for verifying a security of a service operation, comprising:

- a sending unit configured to send a creditability analysis instruction of the service operation to a service terminal in response to an operation request associated with the service terminal;
- a receiving unit configured to receive a creditability analysis result sent by the service terminal, wherein the creditability analysis result is obtained by the service terminal based on the service terminal performing a creditability analysis of the service operation and one or more risk control models pre-stored in the service terminal; and
- a verifying unit configured to determine the security of the service operation based on the creditability analysis result.

14. A terminal, comprising:

- a memory configured to store a set of instructions;
- a processor configured to execute the set of instructions to cause the terminal to:
 - generate one or more risk control models based on user data associated with a user of the terminal;
 - receive a creditability analysis instruction of a service operation sent by a service server in response to an operation request associated with the terminal;
 - obtain a creditability analysis result of the service operation based on the service terminal performing a creditability analysis and the one or more risk control models pre-stored in the terminal; and
 - send the creditability analysis result to the service server for determining a security of the service operation.

15. A service server, comprising:

- a memory configured to store a set of instructions;
- a processor configured to execute the set of instructions to cause the service server to:
 - send a creditability analysis instruction of a service operation to a service terminal in response to an operation request associated with the service terminal;
 - receive a creditability analysis result sent by the service terminal, wherein the creditability analysis result is obtained by the service terminal based on the service terminal performing a creditability analysis of the service operation and one or more risk control models pre-stored in the service terminal; and
 - determine a security of the service operation based on the creditability analysis result.

16. A non-transitory computer readable medium that stores a set of instructions that is executable by at least one processor of a service terminal to cause the service terminal to perform a method for verifying a security of a service operation, the method comprising:

- generating one or more risk control models based on user data associated with a user of a service terminal;
- receiving a creditability analysis instruction of the service operation, the creditability analysis instruction being sent by a service server in response to an operation request associated with the service terminal;

obtaining a creditability analysis result of the service operation based on the service terminal performing a creditability analysis and the one or more risk control models pre-stored in the service terminal; and

sending the creditability analysis result to the service server for determining the security of the service operation.

17. The computer readable medium according to claim 16, wherein the set of instructions that is executable by the at least one processor of the service terminal to cause the service terminal to further perform:

obtaining the user data from the service terminal based on an authorization permission of the user of the service terminal;

generating the one or more risk control models by analyzing the user data; and

storing the one or more risk control models in a database of the service terminal.

18. The computer readable medium according to claim 17, wherein the set of instructions that is executable by the at least one processor of the service terminal to cause the service terminal to further perform:

encrypting the one or more risk control models before storing the one or more risk control models in a local security control database of the service terminal; and

storing the encrypted one or more risk control models in the database of the service terminal.

19. The computer readable medium according to claim 17, wherein the user data comprises at least one of: user social data, interest data and habit data, and wherein the one or more risk control models comprise at least one of: a social relationship control model generated based on the user social data, an interest control model generated based on the interest data, and a habit control model generated based on the habit data.

20. The computer readable medium according to claim 16, wherein obtaining a creditability analysis result of the service operation comprises:

obtaining service information of the service operation based on the creditability analysis instruction;

obtaining a target risk control model from the one or more risk control models based on a type of the service operation, wherein the one or more risk control model includes a corresponding relationship between the service information and service creditability analysis values; and

searching the target risk control model by using the service information as a keyword to obtain a service creditability analysis value corresponding to the service information.

21. The computer readable medium according to claim 20, wherein obtaining service information of the service operation based on the creditability analysis instruction comprises:

obtaining the service information from the creditability analysis instruction of the service operation, wherein the service information includes information obtained by the service server based on the operation request of the service operation sent by another terminal.

22. The computer readable medium according to claim 20, wherein the set of instructions that is executable by the at least one processor of the service terminal to cause the service terminal to further perform:

when the user of the service terminal initiates the service operation, sending the operation request of the service operation to the service server before receiving the creditability analysis instruction; and

when receiving the creditability analysis instruction, obtaining the service information of the service operation based on the operation request of the service operation.

23. A non-transitory computer readable medium that stores a set of instructions that is executable by at least one processor of a service server to cause the service server to perform a method for verifying a security of a service operation, the method comprising:

sending a creditability analysis instruction of the service operation to a service terminal in response to an operation request associated with the service terminal;

receiving a creditability analysis result sent by the service terminal, wherein the creditability analysis result is obtained by the service terminal based on the service terminal performing a creditability analysis of the service operation and one or more risk control models pre-stored in the service terminal; and

determining the security of the service operation based on the creditability analysis result.

24. The computer readable medium according to claim 23, wherein the set of instructions that is executable by the at least one processor of the service server to cause the service server to further perform:

before sending the creditability analysis instruction to analyze the creditability of the service operation to the service terminal, receiving the operation request of the service operation sent by another terminal; and

obtaining service information of the service operation based on the operation request, wherein the creditability analysis instruction of the service operation includes the service information of the service operation.

25. The computer readable medium according to claim 23, wherein the set of instructions that is executable by the at least one processor of the service server to cause the service server to further perform:

before sending the creditability analysis instruction of the service operation to the service terminal, receiving the operation request of the service operation sent by the service terminal, wherein the operation request is used as a trigger instruction for sending the creditability analysis instruction of the service operation to the service terminal.

26. The computer readable medium according to claim 23, wherein determining the security of the service operation based on the creditability analysis result comprises:

obtaining a first creditability analysis value of the service operation based on a local risk control model;

obtaining a second creditability analysis value based on the creditability analysis result sent by the service terminal;

obtaining weight values of the first creditability analysis value and the second creditability analysis value;

calculating a combined creditability analysis value of the first creditability analysis value and the second creditability analysis value based on the weight values;

comparing the combined creditability analysis value with a preset creditability threshold; and

if the combined creditability analysis value is greater than the creditability threshold, determining that the service operation is secure, and if the combined creditability analysis value is not greater than the creditability threshold, determining that the service operation is insecure.