CLAIMS

1. A method for controlling service operation risks, wherein the method comprises:

monitoring, by an application program installed locally on an end-user device, a service operation initiated by a user for invoking offline service information to complete an offline service, the offline service comprising a transaction initiated by a user of the end-user device in an offline environment (S101);

retrieving, by the application program, recorded historical operation data associated with the end-user device from a log file that is stored locally on the end-user device;

determining, by the application program, whether the service operation is a risky operation based on the recorded historical operation data locally retrieved from the end-user device and at least one of a predetermined risk evaluation rule or a risk evaluation model (S102);

in response to determining that the service operation is a risky operation, refusing to invoke the offline service information (S103); and

in response to determining that the service operation is not a risky operation, invoking, by the application program, the offline service information (S104).

2. The method according to claim 1, wherein determining whether the service operation is a risky operation comprises:

determining a first identity verification operation related to the service operation;

determining a risk characterization value of the first identity verification operation based on a first verification method corresponding to the first identity verification operation, the historical operation data, and at least one of the predetermined risk evaluation rule and risk evaluation model;

determining, based on the risk characterization value and a predetermined risk threshold, whether the risk characterization value exceeds the predetermined risk threshold;

in response to determining that the risk characterization value exceeds the predetermined risk threshold, determining the service operation as a risky operation; and

in response to determining that the risk characterization value does not exceed the predetermined risk threshold, determining the service operation as a non-risky operation.

3. The method according to claim 1, wherein determining whether the service operation is a

risky operation comprises:

determining a first identity verification operation related to the service operation;

determining a risk characterization value of the first identity verification operation based on a first verification method corresponding to the first identity verification operation, the historical operation data, and at least one of the predetermined risk evaluation rule and risk evaluation model;

initiating backup identity verification to the user when the risk characterization value exceeds a predetermined risk threshold, receiving a second identity verification operation performed by the user based on the backup identity verification, determining a risk characterization value of the second identity verification operation based on a second verification method corresponding to the second identity verification operation, the historical operation data, and at least one of the predetermined risk evaluation rule and risk evaluation model, and determining whether the risk characterization value of the second identity verification operation exceeds the predetermined risk threshold, in response to determining that the risk characterization value of the second identify verification operation exceeds the predetermined risk threshold, determining the service operation as a risky operation; in response to determining that the risk characterization value of the second identify verification operation does not exceed the predetermined risk threshold, determining the service operation as a non-risky operation; and

determining the service operation as a non-risky operation when the risk characterization value does not exceed a predetermined risk threshold.

4. The method accordingly to claim 2 or claim 3, wherein the first identity verification operation comprises an identity verification operation performed by the user after a previous time the user passes identity verification of the application and before the user performs the current service operation.

5. The method according to claim 3, wherein initiating backup identity verification to the user comprises:

selecting a second identity verification method from a predetermined identity verification method based on the first verification method and at least one of the predetermined risk evaluation rule and risk evaluation model; and

initiating backup identity verification to the user by using the selected second identity verification method.

6. The method according to any one of claims 1 to 5, wherein recording historical operation data comprises:

monitoring an operation performed by the user on the application program; and

determining operation data corresponding to the operation after the operation is monitored, and recording the operation data as the historical operation data; wherein

the historical operation data comprises at least one of a total number of times of identity verification success or failure in a historical time, a number of times of identity verification success or failure within a predetermined time period, behavior data of using an online service by the user, behavior data of using an offline service by the user, and service environment data.

7. The method according to claim 1, wherein offline service information comprises information needed for performing an offline service, including user account information and a service verification identifier, and wherein the offline service information takes the form of a near field communication (NFC) signal, a unique digital object identifier (DOI), or a sound wave signal.

8. The method according to claim 1, wherein the risk evaluation rule and the risk evaluation model can also be dynamically adjusted based on a use environment of the application. The use environment can include time of using the application, a number of times of starting and stopping the application.

9. The method according to claim 1, wherein prior to invoking the offline service information, the method comprises obtaining historical operation data of previous operations performed by the user.

10. The method according to any one of claims 1 to 9, wherein:

the application program on the end-user device comprises client software;

the service operation initiated by the user comprises an offline payment operation;

refusing to invoke the offline service information comprises rejecting the offline payment operation; and

invoking the offline service information comprises performing the offline payment operation.

11. A device for controlling service operation risks, wherein the device comprises multiple modules configured to perform the method of any one of claims 1 to 10.